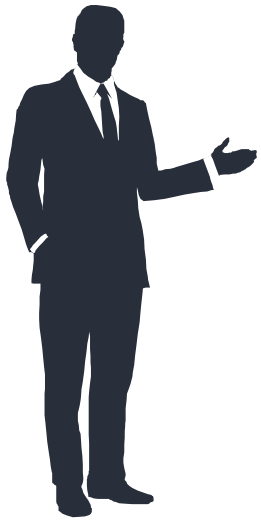
資安規範宣導

本國銀行資安監理重點說明

金管會銀行局

107年2月5日

報告大綱



壹 背景說明

貳 銀行資訊安全相關規範

參 資訊安全防護措施

肆 資安相關措施未完成改善之銀行，應採行因應措施並限期完成

伍 其他應配合事項

陸 近期資安事件處理情形

柒 未來工作重點

捌 結論

壹、背景說明

- 隨著資通訊科技之發展及各銀行陸續推動數位化金融環境，引進金融科技(Fintech)為未來發展趨勢，銀行面臨之資安風險亦逐漸提高。
- 銀行應採行相關措施以提升資安防護能力，確保資訊安全。

貳、銀行資訊安全相關規範

- 依據「金融控股公司及銀行業內部控制及稽核制度實施辦法」第38條規定，銀行業應對業務或交易、資訊交互運用等建立資訊安全防護機制及緊急應變計畫。
- 本會已督導銀行公會訂定相關安控規範，供金融機構遵循，並請公會配合國內外資安發展，適時修正。

貳、銀行資訊安全相關規範(續)

- **銀行公會資安自律規範：**

1. 金融機構資訊系統安全基準
2. 金融機構辦理電子銀行業務安全控管作業基準(電子銀行安控基準)
3. 金融機構辦理電腦系統資訊安全評估辦法
4. 金融機構運用新興科技作業規範
5. 金融機構辦理自動櫃員機資訊安全攻防演練計畫

貳、銀行資訊安全相關規範(續)

- 銀行公會資安自律規範：

6. 金融機構提供自動櫃員機系統安全作業規範
7. 金融機構提供行動裝置應用程式作業規範
8. 金融機構提供QR Code掃描支付應用安全控管規範
9. 銀行業分散式阻斷服務(DDoS)防禦與應變作業程序
10. 金融機構辦理行動金融卡安全控管作業規範
11. 金融機構辦理資訊安全滲透測試計畫

銀行公會資安自律規範-近期修訂重點

自律規範	增修重點
金融機構辦理自動櫃員機資訊安全攻防演練計畫(105年10月訂定)	委由外部機構依所訂演練狀況進行攻擊，俾發現ATM資安威脅與弱點
金融機構提供自動櫃員機系統安全作業規範(106年2月訂定)	就ATM應用程式開發、測試與派版、系統架構區隔與存取限制、汰換計畫、日常監控警示及資安防護與演練等項目予以規範，以強化ATM資安防護

銀行公會資安自律規範-近期修訂重點

自律規範	增修重點
金融機構提供行動裝置應用程式作業規範(106年6月修正)	參照經濟部工業局「行動應用APP基本資安自主檢測推動制度」，每年委由專業機構完成安全檢測，並增訂專業機構檢測人員之資格條件
運用新興科技作業規範(106年8月修正)	增訂生物特徵資料之安全控管機制

銀行公會資安自律規範-近期修訂重點(續)

自律規範	增修重點
金融機構提供QR Code掃描支付應用安全控管規範(106年8月訂定)	1. 明定QR Code訊息傳輸安全及應用程式設計要求 2. 收款跟付款不能使用同一組QR Code，應以專碼專用為原則 3. 由付款客戶行動裝置產生供收款單位掃描之QR Code(被掃模式)，應限定使用時效且最多僅能使用一次，以避免QR Code被攔截
銀行業分散式阻斷服務(DDoS)防禦與應變作業程序(106年10月訂定)	1. 規範透過檢視內部防護資源，依防護設備所提供服務，建置多層次防護機制，並規範事前準備、事中應變及事後處置之防護作為 2. 銀行業者應以本作業程序為基礎，規劃符合自身提供服務與需求之DDoS防禦與應變程序書

銀行公會資安自律規範-近期修訂重點(續)

金融機構辦理行動金融卡安全控管作業規範(106年12月訂定)

- 定義行動金融卡係透過空中傳輸下載個人化資料至行動裝置，發行具行動交易功能之金融卡
- 明定行動金融卡分類及申辦作業之控管規定：

行動金融卡	應用範圍
第一類(即晶片金融卡)	轉帳、提款、消費交易
第二類(即Visa Debit卡等)	僅限於消費交易

- 明定亂碼化作業、行動裝置端之金鑰管理作業，以及應用系統之控管規定

銀行公會資安自律規範-近期修訂重點(續)

金融機構辦理資訊安全滲透測試(107年1月訂定)

- 測試範圍：委由外部專業機構對金融機構提供網際網路服務之網站，辦理營運區、測試區、辦公區等不同環境之滲透測試
- 辦理期程：107.3.15完成

本會已要求測試結果及缺失改善方案提報董事會後，107年4月底前函報本會

銀行公會資安自律規範-近期修訂重點(續)

電子銀行安控基準(修正草案報會，刻正審核中)

- 新增Account Link規範：
  客戶透過電子銀行(如網銀、全國繳費網)、授權事業單位或其他金融機構發動交易指示，直接由客戶帳戶扣款至指定帳戶

- 修正線上辦理授信業務之安全設計：
  修正數位存款帳戶及信用卡客戶線上辦理授信業務簽約對保之相關安全設計

銀行公會資安自律規範-近期修訂重點(續)

金融機構使用物聯網設備安全控管規範
(修正草案報會，刻正審核中)

- **規範重點：**

  明定應建立具網路連線功能之物聯網設備安全更新機制、使用者之身分驗證機制、應關閉不必要之網路連線及服務等安控要求，並訂定例外處理情形

參、資訊安全防護措施

每年將資安執行情形提報董事會

- 每年第一季前，將前一年度資安整體執行情形提報董事會，內容包括相關函示與資安規範之遵循情形、資訊安全防護機制與緊急應變計畫等執行情形

設置資安專責部門及主管

- 應設置資安專責單位及相當層級之專責主管
- 配置適足人力及資源，以有效執行資安防護工作
- 逐步將資安專責單位提升至獨立專責部門，以維持其執行資安業務之獨立性

肆、資安相關措施未完成改善之銀行，應採行因應措施並限期完成

ATM攻防演練缺失事項之改善

- 105年各金融機構辦理ATM攻防演練所發現之缺失事項，仍有少數銀行未完成改善，應請採行相關因應措施，並於106年底前完成改善，107年2月底前將相關辦理情形函報本會

強化APP資安

- 本會已請各銀行參照經濟部工業局「行動應用APP基本資安規範」，委由專業機構完成對現行所有APP之全面安全檢測
- 部分銀行之APP未能符合上開規範，應採行因應措施，並於106年底前完成改善，107年2月底前將相關辦理情形函報本會

肆、資安相關措施未完成改善之銀行，應採行因應措施並限期完成(續)

完成ATM-EMV晶片化作業

- ATM無法讀取國際卡EMV晶片資料而改以磁條交易發生偽卡交易損失，將由ATM所屬金融機構承擔
- 尚未完成跨國提款ATM-EMV晶片化作業之銀行，宜儘速完成，以降低跨國提款承受偽卡損失風險：
  - 可採軟體升級之ATM，106年底前完成
  - 無法採軟體升級之ATM，107年底前汰換完成，並優先設置無障礙ATM

伍、其他應配合辦理事項

銀行於紐約設有分支機構，總行應督導及協助其確實遵循美國紐約州金融署(DFS)網路安全相關規範

- DFS公布「金融服務業網路安全規範」(Part 500)，要求建立並維護網路安全計畫
- 請相關銀行總行督導及協助其紐約地區分行確實遵循
  - 簽署及提交符合網路安全規範聲明書前，至少應由總行進行一次查核訪談，以確保相關作業均已符合DFS規定
  - 聲明書提交前，宜向DFS表達可親向該署簡報有關「Part500簽署準備情形」，以協助DFS對整體法遵內容及執行情形有所瞭解。

伍、其他應配合辦理事項(續)

遵循銀行公會相關資安自律規範

- 為因應並防範相關資安風險，本會已請銀行公會訂定相關資安自律規範，並配合資安現況適時修正，請各銀行務必遵循辦理

持續辦理或派員參加資安事件研討會

- 本會已督導銀行公會辦理資安事件防護研討會，及資安規範說明會
- 未來仍請銀行公會視國內外資安狀況，持續辦理研討會，各銀行應請派員參加

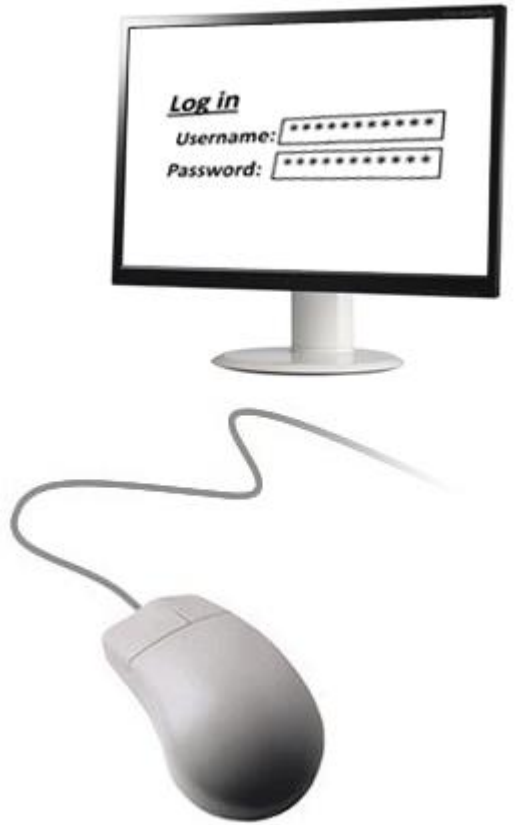
伍、其他應配合辦理事項(續)

連續假期資訊系統安全維護機制

- 應確實建立系統及資安監控機制，應變計畫與通報程序，並進行情境演練
- 應特別注意各類異常情形之監控，包括特權帳號使用、資訊系統異動、防毒防駭事件警訊、internet存取紀錄、派版軟體及病毒碼更新設備等之監控處置，並將不必要系統關機
- 原則禁止遠端連線(禁止由外部連線至銀行內部營運區進行系統維護作業)，如有緊急需要，應加強監控管理，例如身分驗證、授權人工確認等

陸、近期資安事件處理情形-ATM盜領案

- 國內銀行發生ATM盜領案後，本會已採行下列措施：
  - 請各金融機構對個案相同機型ATM加強檢測、強化ATM監控機制及應變處理能力，並加強總行與海外分(子)行連線及銀行內網之控管機制
  - 請銀行公會檢視該會相關自律規範之周全性及妥適性



陸、近期資安事件處理情形-ATM盜領案

請各銀行辦理下列事項：

(1)105年底完成ATM資訊安全之攻防演練

(2)請外部資安團隊針對與客戶相關之ATM及網路銀行系統進行電腦系統資訊安全評估作業

陸、近期資安事件處理情形-SWIFT系統遭駭客入侵

1. 個案發生原因

106.9.11

入侵銀行內部網路環境

竊取多組權限帳號➔掌握該行網路環境

潛伏期

106.10.3
（中秋節前一天）

- 發動攻擊：短時間內入侵大量電腦伺服器
- SWIFT系統植入惡意程式後，取得銀行內部相關交易資料，並竄改交易資料密文，如：受款人及金額，發送偽冒匯款電文給國外通匯行，轉帳至駭客指定戶頭，同時散布大量勒索軟體與破壞系統，以混淆該行注意力並消除其行為軌跡

106.10.5

- 確認遭盜轉虛偽跨境交易
- 將終端伺服器等相關電磁明細提供刑事警察局追查
- 刑事警察局協助數位鑑識還原工作，釐清駭客入侵手法及途徑，並追查來源

陸、近期資安事件處理情形-SWIFT系統遭駭客入侵

2.銀行應變及改善措施

- 將SWIFT系統進行實體隔離，並強化SWIFT交易之內控機制。
- 同時委託第三方專業資安管理與技術管理顧問公司，全盤檢討現行網路安全防禦，強化防火牆及入侵偵測系統等資安設備。

陸、近期資安事件處理情形-SWIFT系統遭駭客入侵

3.本會採行措施

- 106年10月6日
  - 經清查其他本國銀行(含外商銀行在台分行)SWIFT系統均屬正常
  - 因應連續假期金融機構資訊系統作業安全，已通知各金融機構：
    1. 加強各類異常情形之監控
    2. 原則禁止遠端連線
    3. 交易金額大於一定金額以上者，要求call back確認
    4. 就本次駭入病毒進行檢測掃毒

陸、近期資安事件處理情形-SWIFT系統遭駭客入侵

3.本會採行措施(續)

- 請銀行公會研議修正相關規定：
  - 修正「金融機構辦理電腦系統資訊安全評估辦法」，將SWIFT系統納入每年評估範圍，並委由外部專業機構進行安全檢測。
  - 研議強化相關環境架構之具體可行作法，評估調整完成期程，並配合修正「金融機構資訊系統安全基準」。
- 請金融機構務必瞭解SWIFT客戶資安計畫(CSP)檢測項目內容，並於期限內完成CSP各項檢測，相關檢測結果將納為本會監理及相關業務准駁之參考。

SWIFT Customer Security Programme

柒、未來工作重點

加強金融監理與資訊安全之結合

- 將資訊安全辦理情形納入金融業者申辦業務准駁考量因素。
- 資訊安全納為存款保險費率計提之因素。
- 研議將資訊安全辦理情形納入作業風險資本計提之考量。

推動金融業資安聯防體系

- 藉由「金融資安資訊分享與分析中心（F-ISAC）」，分享、通報資安風險，避免金融業遭受連環資安攻擊
- 請銀行業儘速加入成為會員

研訂「金融控股公司及銀行業內部控制及稽核制度實施辦法」第38條之1有關資安相關規定

資安專責單位及主管	• 設置資安專責單位及主管，不得兼任資安以外其他工作 • 資產規模一兆元以上，應設置具職權行使獨立性之資安專責單位，並指派協理以上人員擔任主管 • 資安專責單位應將資安整體執行情形提報董事會 • 資安專責單位主管應與董事長、總經理、總稽核聯名出具資安聲明書
教育訓練	• 資安專責單位人員，每年至少應接受15小時以上資安專業課程訓練或資安職能訓練 • 其他人員每年至少須接受3小時以上資安宣導課程
同業公會職責	• 應訂定並定期檢討資訊安全自律規範

捌、結論

- 本會就銀行業內部控制及稽核制度已有相關規範，並請銀行公會訂定相關安控自律規範，以供金融機構遵循。為強化資安控管，本會已研修內部控制及稽核制度實施辦法，將資安規範予以法制化。
- 金融機構應提升對資安之重視，確實落實執行相關規範，以提升資安防護能力。
- 本會將持續注意國內外資安狀況，採取適當措施，以強化資訊安全，維持金融市場之穩定。

以上報告
謝謝大家