主題三

本國銀行相關資安風險認知及資安資訊分享

檢查局

107年2月5日

- 金融資安風險
- 銀行資訊作業查核發現
- 新興科技風險管理

營運持續的威脅與衝擊

影響企業持續營運前五大威脅、衝擊和趨勢

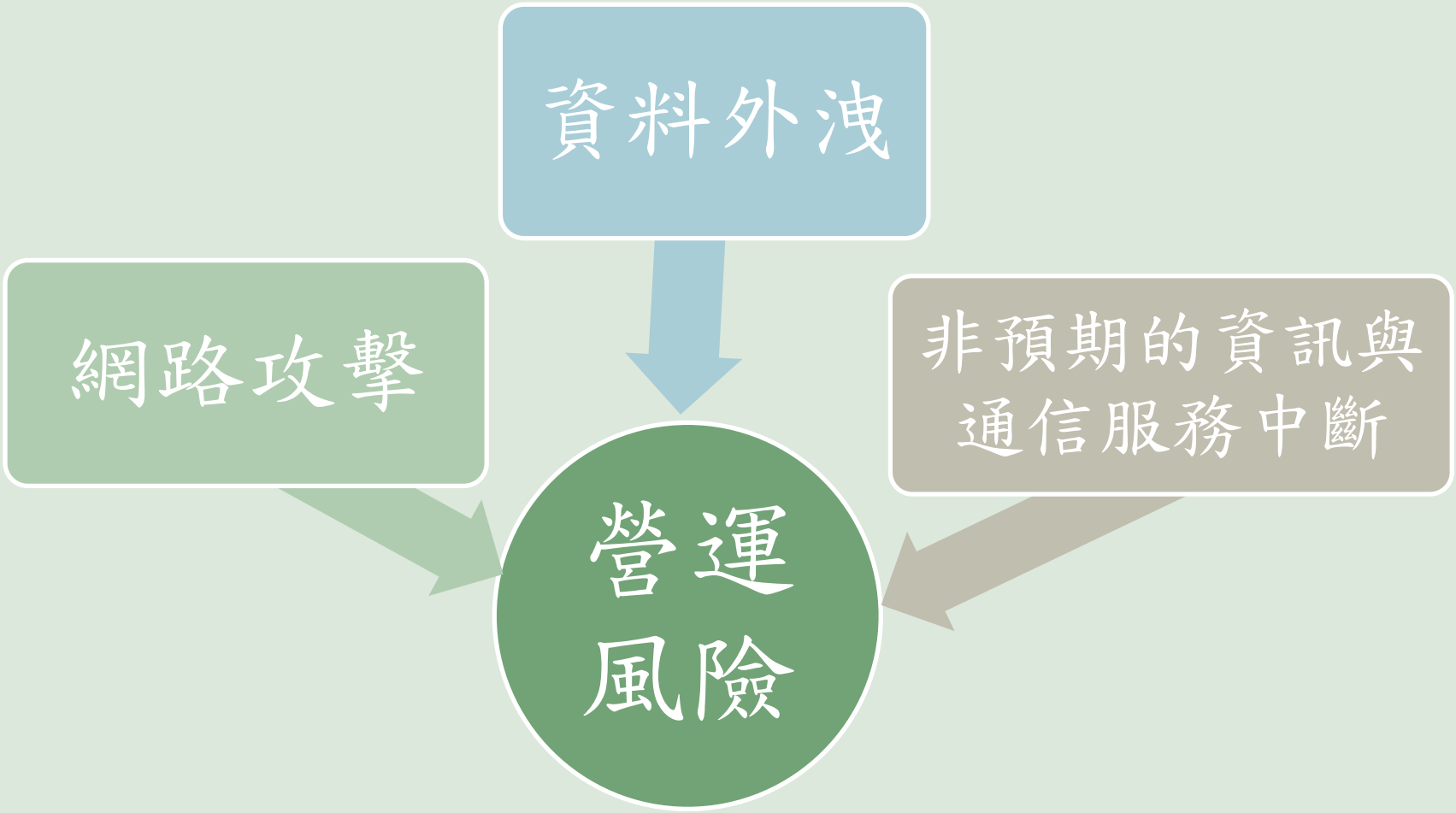
	威脅（Threats）	衝擊（Disruptions）	趨勢（Trends）
第一名	網路攻擊	無預警的資訊與通訊中斷	使用互聯網進行惡意攻擊
第二名	資料外洩	惡劣氣候	社群媒體的影響
第三名	無預警的資訊與通訊中斷	公共服務中斷	流失重要員工
第四名	安全事故	網路攻擊	新法規和更嚴謹的監管審查
第五名	惡劣氣候	安全事故	互聯網相關服務的普及和高度採用

資料來源：英國持續營運管理協會，2017年5月

資料來源：iThome網站-106.5.25【資安周報第72期】

金融資安風險

資訊安全是威脅金融業運作的重大因素



近期國際金融資安訊息

- 俄羅斯資安業者Group-IB於2017/12/11發布訊息，一俄國駭客組織一年來入侵銀行轉帳網路，至少18家美國、俄羅斯銀行遭自ATM盜領現金近1000萬美元。（國家資通安全會報技術服務中心2017/12/26資安新聞）

- 美國兩大ATM製造商NCR與Diebold Nixdorf近期向美國金融機構發出警告，ATM自動吐鈔的jackpotting攻擊手法已蔓延到美國。（iThome網站2018/1/29 資安新聞）

- 美國電信商Verizon發布2017年資料外洩調查報告顯示，社交工程網路釣魚手法，是駭客使用率最高的伎倆，透過電子郵件傳播惡意軟體的比例高達93.8%。（iThome網站2018/1/21 資安新聞）

我國金融資安環境風險

銀行SWIFT系統遭駭客發送假交易指示

ATM遭植入吐鈔惡意軟體

透過社交工程、網路釣魚或木馬程式竊取客戶個資

網路環境攻擊

行動裝置APP遭駭

阻斷式攻擊癱瘓交易系統

冒用帳號密碼並跳脫防火牆機制讀取營運資料庫

銀行資訊作業查核發現(1/2)

✓ 常見缺失

防火牆機制	網路系統漏洞檢測	帳密等系統參數設定管理
email安控	APP交易安全設計	監控條件完整性
個資控管盤點與演練	正式與測試環境區隔控管	軌跡留存與覆核
USB控管	VPN控管	帳密權限與控管

銀行資訊作業查核發現(2/2)

✓ 現行安控機制弱點

- » 對法規之遵循及落實情形明顯不足
- » 自傳統獨立系統轉變為開放式之網路交易環境，未能意識其受駭弱點之演進風險

現有資安控管機制已不敷因應駭客滲透手法

主要資安規範(1/3)

✓ 銀行業務

- 金融機構資訊系統安全基準
- 金融機構辦理電腦系統資訊安全評估辦法
- 金融機構提供行動裝置應用程式注意事項
- 金融機構辦理電子銀行業務安全控管作業基準
- 銀行受理客戶以網路方式開立數位存款帳戶作業範本
- 金融機構辦理自動櫃員機資訊安全攻防演練計畫
- 金融機構提供ATM系統安全作業規範
- 金融機構自動櫃員機安全防護準則

主要資安規範(2/3)

✓信用卡業務

- 信用卡收單機構簽訂「提供代收代付服務平台業者」為特約商店自律規範
- 信用卡業務機構辦理手機信用卡業務安全控管作業基準
- 中華民國銀行公會「辦理信用卡業務機構防制洗錢及打擊資助恐怖主義注意事項範本」

✓電子支付業務

- 電子支付機構資訊系統標準及安全控管作業基準辦法
- 與境外機構合作或協助境外機構於我國境內從事電子支付機構業務相關行為管理辦法

主要資安規範(3/3)

✓ 新興科技

- 運用新興科技應注意事項
- 金融機構提供行動裝置應用程式作業規範
- 使用電子銀行(網路銀行及行動支付)應注意事項
- 透過網際網路傳遞金融交易訊息之網路應用系統，除應遵循「金融機構辦理電子銀行業務安控作業基準」，應同時遵循金融憑證網路應用系統開發注意事項
- 信用卡業務機構辦理手機信用卡安全控管作業基準
- 行動應用APP基本資安規範

新興科技風險管理(1/2)

✓ 雲端計算(Cloud Computing)

» 明確訂定雲端服務供應商合約，要求具備資安管理機制，如資料安全保護策略、安全認證、交易安全設計、實體安全、備援及稽核等，並確認資安事件之責任範圍

✓ BYOD(Bring Your Own Device)

» 訂定BYOD政策及管理規範，以防止資訊意外洩露、暴露員工或客戶隱私。

✓ 社群媒體(Social Media)

» 以嚴謹態度評估社群媒體之使用，據以制定策略及管理規範，以避免資料外洩、假冒或貶損性資訊、暴露於惡意程式攻擊標的、社交工程等其他安全威脅。

所衍生之科技風險包括網路攻擊、資料外洩、營運中斷等

新興科技風險管理(2/2)

✓ 委外作業管理

- 因應金融數位化發展，金融機構多與資訊服務廠商策略合作開發程式，對廠商開發完成之程式，應建立妥適之測試及驗收程序加強管理，以確保系統執行之正確性
- 部分銀行對委外廠商開發完成之程式，僅由作業單位簡要測試後即上線，造成寄送客戶之交易內容夾帶非本人之交易資料，導致資料外洩

➡ 應善盡對委外廠商之監督管理

結語(1/2)

✓ 因應金融科技創新–現行作業

» 強化資訊作業及網路安全基礎措施

落實由三道防線(各部門資訊作業、法遵及稽核)確認遵循資訊系統安控基準等相關規定，強化資訊與網路基礎建設

» 建立重大資安事件通報機制

檢討現行資安事件通報流程之即時性及處理程序之有效性，並落實資安演練

結語(2/2)

✓ 因應金融科技創新-未來方向

» 強化資安風險管理

- ✓ 提升資安治理層級，重視資安專責組織
- ✓ 重視業務擴展，重行評估資安人力配置
- ✓ 將資安納入風險指標
- ✓ 強化數位、即時監控系統
- ✓ 建立數位鑑識作業程序
- ✓ 提升員工資安意識

感謝聆聽