臺灣期貨交易所
TAIWAN FUTURES EXCHANGE

106年資通安全宣導

活絡期貨交易 服務實質經濟

避險增益 價格發現

臺灣期貨交易所

106年2月

資通安全宣導(一)

- 雲端、社群、行動裝置資訊之管控措施
  - 為強化期貨業運用雲端運算服務、社群媒體及行動裝置之資訊安全，期貨公會特訂定「雲端運算、社群媒體、行動裝置資訊安全自律規範」，並於106年1月4日以中期商字第1050006071號函公告。
  - 自律規範主要內容分別有目的、定義、資訊安全法令遵循、雲端運算服務運作安全、社群媒體安全控管、行動裝置安全控管、違規之處理、附則等8條。
  - 請業者洽期貨公會網站

資通安全宣導(二)

- 證券暨期貨產業資安資訊分享與分析平台 SFISAC
  - 營運目的：建立資安聯防機制
  - 分享資安資訊：即時取得GISAC與其他資安組織分享之資安情資，及所屬會員資安事件資料，分享資安資訊。
  - 加強防護意識：透過資安資訊分享方式，提升會員資安相關知識並加強證券與期貨市場整體資安防護意識。
  - 預防事件擴大：藉由應變處理及通報程序，進行事件分析、鑑識、排除與追蹤處理，掌握發生資安事件相關資訊和協助解決問題，防範資安事件蔓延擴大。
  - 網址： ***https://fisac.twse.com.tw/***
  - 該平台係採會員制，請業者透過上開網址申請入會，期能取得相關資源。

資通安全宣導(三)

- 資安新威脅與資訊科技發展評估分享
  - 2016全球資安發展趨勢
    - 物聯網設備安全之需求迫切
    - 勒索軟體與犯罪團體氾濫
    - 關鍵基礎設施之網路攻擊嚴重化
    - 生物識別將廣泛應用
    - 對 IOS設備攻擊將更多
    - 網路攻擊與資料外洩推動網路保險需求
    - 更強的加密需求
    - 安全的遊戲機制將出現巨大需求

資通安全宣導(四)

- 近期資安事件分享
  - 舊金山輕軌系統遭遇勒索軟體攻擊
    - 事件：美國舊金山市交通局（San Francisco Municipal Transportation Agency）2016/11/26傳出遭到駭客入侵，員工的電腦螢幕上出現「你已被駭」（You hacked）的字樣，輕軌的售票系統失靈，使得當局一度開放票閘出入口讓乘客免費進出以減少對交通的衝擊。（iThome ： 2016-11-28）
    - 原因：電腦系統脆弱性管理失效、安全漏洞未修補。
  - Tesco銀行遭駭事件
    - 事件：遭到駭客盜領存款的英國Tesco Bank，遭到盜領總計有約9000個帳戶，共計250萬英鎊（約合新台幣9725萬元）。Tesco Bank表示，用戶的個人資料並未在攻擊中外洩，該行並已經針對遭盜領的帳戶將被盜款項歸還給持有人，而一度暫停近2天的線上簽帳轉帳服務，亦已恢復正常。
    - 原因：電腦系統安全防護弱點、惡意軟體感染。

資通安全宣導(五)

- 針對整體資通環境、以風險管理為核心之管理專法
  - 資通安全管理法草案

第一章總則 §1 ～§8	立法目的、名詞解釋、資通安全產業之推動、行政院職責、幕僚任務委任或委託、資安責任等級分級、情資分享機制、資通委外監督
第二章公務機關資通安全管理 §9 ～§14	資通安全管理與維護計畫、資通安全長之設置、年度資通安全報告之提出、資通安全查核通報應變措施、獎懲措施
第三章非公務機關資通安全管理 §15 ～§18	關鍵基礎設施提供者資通安全維護之管理與監督、受指定之非公務機關所提供之產品或服務資通安全管理之管理與監督、資通安全事件通報應用行政檢查
第四章罰則 §19 ～§22	行政處分
第五章附則 §23 ～§24	施行細則授權、施行日期

資通安全宣導(六)

- 強化重要系統及設備資安機制（重申內控），例如：
  - 對重要系統及設備應定期辦理資訊安全風險評鑑，並留存紀錄。
  - 應定期評估自身網路系統安全。
  - 應定期或適時修補網路運作環境之安全漏洞。
  - 重要網站及伺服器系統應以防火牆與外部網際網路隔離。
  - 安裝防毒軟體，並及時更新程式及病毒碼、對電腦系統及資料儲存媒體進行病毒掃瞄、防毒應涵蓋個人端（含攜帶型及營業處所內供投資人共用之電腦等）及網路伺服器端電腦。
  - 每半年至少應執行網路系統外部弱點掃瞄作業乙次。
  - 委外作業人員應納入公司安全管理，欲使用內部網路資源時應有安全管制措施(如實體隔離)。

資通安全宣導(七)

- 可再強化資安防護事項（主管機關期許）：
  - 針對風險性較高之攻擊手法如SWIFT弱點攻擊、APT攻擊及勒索軟體等加強防護及宣導：如宣導針對特定組織所作的複雜且多方位的網路攻擊及勒索軟體感染方式，並進行設交工程演練 。
  - 增加資源分配於資訊軟硬體升級及強化資安防護能量：如 增加資安維護人力及資安軟硬體設備之預算。
  - 如有使用微軟公司之目錄服務、作業系統或開發環境，應有更嚴格之控管措施，並更新修補程式：如收回個人電腦管理者權限、設定自動windows update等。
  - 除應強化相關規範及措施外，更應嚴格要求承辦人員落實執行相關資安規範：如定期資安宣導或公告重申相關規定。

資通安全宣導(八)

- 系統開發維護應注意事項
- 目的：確保系統程式功能正確無誤，避免因程式功能不完整造成系統異常或發生相關違規（例如： 持有部位超限、未檢查保證金或保證金計算錯誤等）。
- 期貨商方面
  - 系統測試：
    - 訂定測試計畫，其內容至少包含測試目的、測試完成標準、測試方法及測試記錄格式。
    - 依測試計畫請應用系統使用單位共同測試，記錄所有測試經過及結果。
    - 製作測試報告其內容至少需包含測試目的、測試方法、測試記錄及測試結果總評及建議。
    - 自營相關電腦（主機）及系統應有專人控管，並比照交易系統之軟硬體維運管理。
    - 不得利用客戶帳戶為實境測試