【專題一】

淺談證券商資通安全管理

侯明昊（證期局科員）

壹、前言

隨著資訊科技的發展，金融科技的應用及客戶數據的分析成為金融產業的競爭優勢，為使金融中介機構經營策略不僅侷限於傳統功能，並能有效利用更前瞻性的數位科技協助金融產業多元創新發展，金融監督管理委員會（以下簡稱金管會）致力推動資本市場數位轉型，陸續發布「金融科技發展路徑圖」及「資本市場藍圖」等政策，其中針對證券商之措施包括優化線上開戶、協助證券商發展虛擬據點、推動證券期貨業公開資料查詢之開放證券等措施，以使證券商利用科技深化金融服務。

除受金融科技發展的影響，因應新冠疫情，為降低群聚感染，證券商採行「異地辦公」、「居家辦公」等遠距離辦公模式，仰賴更多的線上服務，相關統計顯示，目前證券商電子下單比重已達 7 成以上，且投資人採用線上開戶之開戶數比重亦已達 6 成，投資人使用證券商線上服務有逐漸上升之趨勢。雖然線上服務帶來了許多便利之處，卻也伴隨潛在的資安風險，近年來金融產業駭客攻擊事件頻傳、資訊服務異常、及機敏性資料外洩事件仍時有報導，不管是 2017 年的分散式阻斷服務攻擊（Distributed Denial-of-Service, DDoS）事件，或者是 2021 年底證券商受託買賣外國有價證券（複委託）下單

系統遭駭客撞庫攻擊事件（Credential Stuffing）等，均顯示資本市場面臨嚴峻的資安挑戰。

為因應與日俱增的資安威脅，及響應「資安即國安」之國家戰略，金管會觀察國際金融資安情勢、國際金融資安監理趨勢，並檢討現行資安監理政策，提出「金融資安行動方案」，期以四年為期，更為提升金融產業資安能量，以於創新開放金融服務的同時，仍能提供民眾安心便利、穩定不中斷的金融服務，保護金融消費者的財產與隱私，亦為金融科技奠定發展的基石。除前開「金融資安行動方案」外，證券商資通安全管理法令之相關具體執行措施繁多，為使證券商管理階層、從業人員、及投資大眾對金管會之證券商資安監理有更進一步瞭解，本專題謹就證券商重要資安事件回顧、證券商資通安全相關政策及法規、證券市場資通安全治理、未來強化作為及監理重點進行介紹，期使讀者認識證券商資安管理之基本架構。

貳、證券商重要資安事件回顧

一、DDoS 勒索攻擊事件

2017 年初金管會首次接獲多家證券商通報遭受 DDoS 攻擊事件，駭客透過高流量耗盡證券商系統或網路資源，導致其對外網路頻寬滿載，造成公司官方網站或網路下單程式速度緩慢情形，其中有部分業者接獲駭客組織寄發勒索信件要求支付虛擬貨幣，否則將持續發動 DDoS 攻擊。

金管會於第一時間清查所有業者受攻擊情形，並協助業者迅速通報警方，成立緊急應變小組，及請業者隨時注意對外網路資安之維護，加強監控網路系統，另向電信業者申請流量清洗服務，以阻擋攻擊。金管會亦檢討相關資通安全規範，督導中華民國證券商業同業公會（以下簡稱證券商公會）訂定「證券商分散式阻斷服務攻擊（DDoS）防禦與應變作業程序範本」以供會員證券商參考，另定期辦理業者 DDoS 攻擊應變演練作業，使業者熟悉相關緊急應變作業程序。嗣於 2018 年底再次發生多家證券商接獲不同駭客組織之勒索信件及 DDoS 攻擊，業者均能於發現攻擊跡象時，即依相關程序辦理通報及啟用流量清洗服務，網路下單服務均能維持正常運作，顯示證券商已具備 DDoS 攻擊應變能力。

二、撞庫攻擊事件

2021 年下旬數家證券商通報其複委託下單系統遭駭客入侵，且有客戶帳戶遭偽冒

下單港股情事，撞庫攻擊手法主係駭客在網路上利用已外洩之證券商客戶帳號密碼資料，再嘗試登入證券商網站，冒用投資人身分進行交易。

金管會發布新聞稿提醒投資人，為避免遭有心人士惡意盜用帳號從事交易，提醒民眾應提高交易密碼之強度，避免使用容易被猜中之密碼並定期更新，勿將所有需註冊會員之網站都設定同樣的帳號密碼，另避免使用圖書館、網咖、機場等地之公用電腦從事交易及輸入敏感性高的資訊，還有應妥善保存身分證件、網路交易帳號密碼及相關的電子憑證，不宜在開戶證券商以外之網站，提供或共用登入之帳號及密碼或交由他人保管，以免帳號遭冒用下單，損及自身權益。

另金管會督導臺灣證券交易所股份有限公司（以下簡稱證交所）敦促證券商強化3大措施。第一，業者應在網路下單登入落實多因子認證，例如下單憑證、綁定裝置、OTP、生物辨識等機制，強化憑證換發的驗證機制，以確保為客戶本人登入。其次，業者應使用優質密碼設定並進行管控，確實執行密碼輸入錯誤次數達3次者應中斷連線，並加強宣導客戶定期更新使用者密碼。第三，業者應每日針對核心系統的帳號登入失敗紀錄、非客戶帳號登入嘗試紀錄等進行監控及瞭解，分析異常登入原因、異常IP登入時通知投資人，並留存相關紀錄。

三、下單系統不穩定、連線異常事件

因行動裝置普及，投資人現多使用證券商APP進行下單，然近年陸續發生證券商下單系統異常、無法登入、連線緩慢等情事，究其下單系統不穩定之原因，主要有證券商網路設備硬體故障、證券商網路設備承載量不足、APP版本更新、資訊廠商設備異常、電廠跳電、電信廠商網路提供異常、投資人端網路流量不足或設定錯誤等，態樣繁多。

為提升證券商APP下單系統穩定性及資通安全，金管會已請證交所敦促證券商汰換老舊網路設備，優化系統及配置備援電力設備及線路，並提醒倘發生當機致無法下單情事，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，避免糾紛。另證交所修正證券商資安內控相關規範，規定證券商應訂定「營運持續管理計畫」、「系統故障復原作業程序」、「可容忍中斷時間」及「系統可用性」等納入內控落實執行，以強化證券商網路下單服務品質。

惟考量影響證券商電子下單穩定之相關變數眾多，有許多不可抗力因素，尚非證券商可完全管控，為避免僅電子下單方式故障影響投資人交易作業，證券商仍應提供多種下單方式，另投資人亦應瞭解網路交易存有相關風險，應於交易時注意，倘發生下單連

線異常情事，應即聯絡所屬證券商協助處理，以免影響自身權益。

參、證券商資通安全相關政策及法規

一、金管會資通安全相關政策

（一）金融資安行動方案

現任金管會黃主委天牧 2020 年於臺灣資安大會金融安全論壇致詞時說道：「資安重視永遠不嫌多，但資安需成本，怎樣尋求好的分際，讓業者願意做並獲得好的後果，是主管機關需嘗試尋求的平衡。」，雖然我國金融機構資安防護已行之有年也有一定的運作機制，惟鑒於資安威脅日益嚴峻，不能待每次資安事件發生後，再去修補資安規範，爰金管會於 2020 年 8 月 6 日發布「金融資安行動方案」，期能強化金融業資安防護能力，達成安全、便利、營運不中斷目標。

金融資安行動方案分別從強化主管機關資安監理、深化金融機構資安治理、精實金融機構資安作業韌性、發揮資安聯防功能等四個面向切入，提出多項資安措施，以 4 年為期分階段推動，定期檢討成果，並依資安發展趨勢及實務運作情形，調整行動方案內容，期能強化金融機構資安防護能力，達成安全、便利、營運不中斷目標。其中涉及資本市場之具體措施包括推動一定規模證券商設置資安長、鼓勵遴聘具資安背景董事或設置資安諮詢委員會、加強董監事人員資安教育訓練、研議資安風險因子與金融資安監理連結之有效性等，均以陸續實施推動。

（二）資本市場藍圖

經綜合我國資本市場現況及國際發展趨勢，資本市場未來將面對數位化、網路化及行動化的科技發展趨勢，將對金融中介機構之經營環境產生重大影響，另考量數位科技之應用，亦有助於監理機關運用監理科技來強化市場監理與預警，進而保護投資大眾之權益，爰金管會發布資本市場藍圖，並於提升金融中介機構市場功能及競爭力之策略中，納入針對資本市場之資安相關監理措施，包括：1、提升業者資通安全水準，強化網際網路服務安全與 營運不中斷，具體作法有完備資安規範、強化備援機制與演練等。2、強化周邊單位資通安全，例如完備市場關鍵資料保全、導入國際持續營運管理

標準制度等。3、強化證券期貨交易市場網路系統安全，評估及驗證交易市場網路安全，確保市場交易安全及正常運作。

（三）證券期貨業永續發展轉型執行策略

鑒於永續發展已是全球普世價值，為營造健全環境（E）、社會（S）及治理（G）生態、強化中介機構永續經營及善盡企業社會責任，爰參酌聯合國責任投資原則、國際證券管理機構組織（IOSCO）所訂 ESG 與資安方案相關指引或報告，並配合證券期貨產業現況，以「完善永續生態體系」、「維護資本市場交易秩序與穩定」、「強化證券期貨業自律機制與整合資源」、「健全證券期貨業經營與業務轉型」、「保障投資或交易人權益及建構公平友善服務」等 5 大目標，研訂「證券期貨業永續發展轉型執行策略」，以利業者共同推動及強化永續發展經營體系。

經研議歸納出現行證券商面臨之資安挑戰包括因應數位化、網路化時代所帶來之駭客入侵、擋庫事件等資安問題，現行人力及安全防護措施仍有待強化，另證券商資訊服務及系統有集中於特定幾家廠商等情形，一旦遇到系統異常或資安事件，易阻礙正常營運而影響投資人權益。該項政策強化資安之具體措施包括鼓勵金融機構導入國際營運持續管理標準、增加資安人員之人力編制、資安人員取得資通安全專業技術類證照、定期評估核心營運系統及設備，確保營運持續、韌性之能力提報董事會等。

二、金管會及證券周邊單位證券商資通安全相關法規

證券管理法令是主管機關依法行政管理資本市場之依據、維持資本市場穩定的基石，屬證券商及相關從業人員應遵循之最低要求，相關政策之具體執行措施亦會納入法令，考量法規細瑣繁多，本文尚難全面敘述，爰謹梳理介紹有關證券商資通安全相關法令其相關自律規範之重點，俾使業者瞭解並得以遵循。

（一）金管會指定非公務機關個人資料檔案安全維護辦法及證券期貨市場資通安全事件通報應變作業注意事項

1、金管會指定非公務機關個人資料檔案安全維護辦法，是由個人資料保護法授權主管機關訂定，證券商亦屬規範主體之一，該規定主係規定證券商應就制度面訂定相關政策，包括依其業務規模及特性，衡酌經營資源之合理分配，配置管理之人員及相當資源，以訂定與執行其個資檔案安全維護計

畫、應訂定個資安全事故通報及預防機制、應訂定個資之管理程序及措施、電子商務服務系統應落實使用者身分確認、網路安全傳輸加密機制等資安措施、及業者並應定期提出相關自我評估報告等。

2、為利主管機關及相關周邊單位於證券期貨業者發生重大資訊服務異常事件或資通安全事件時，能迅速有效掌握事件資訊，爰制定「證券期貨市場資通安全事件通報應變作業注意事項」，並依該注意事項建立證券商資安通報機制及通報系統，證券期貨業者應於發生影響客戶權益或正常營運之資訊服務異常事件或資通安全事件，應於知悉事件 30 分鐘內至通報系統，辦理初步通報。另亦規範證券期貨市場資安事件之級別，其中最嚴重者為第三級別事件，包括機敏資料外洩、核心系統異常等，最輕者為第一級別事件，例如非核心系統異常等。

（二）證券暨期貨市場各服務事業建立內部控制制度處理準則

證券暨期貨市場各服務事業建立內部控制制度處理準則（以下簡稱證期內控處理準則）主係由證券交易法授權主管機關訂定，為證券期貨業者應訂定相關內部控制制度之法據，該準則第 10 條規定，業者使用電腦化資訊系統處理者，其內部控制制度除資訊部門與使用者部門應明確劃分權責外，至少應包括系統開發及程式修改、程式及資料之存取控制、資料處理、檔案及設備之安全、系統復原計畫制度及測試程序之控制、資通安全檢查等控制作業。另為健全證券商之資安規範，金管會修訂該準則第 36 條之 2 及相關令釋，相關重點如下：

1、建立資安專責制度：

(1) 要求設置資安專責單位及主管：針對不同規模、業務及組織特性之證券商要求配置適當人力資源及設備負責資訊安全制度之規劃、監控及執行資訊安全維護作業，進行差異化管理，其中依證券商實收資本額劃分四個等級，資本額 200 億元以上為第一級證券商、資本額 100 億元以上未達 200 億元為第二級證券商、資本額 40 億元以上未達 100 億元為第三級證券商，資本額 40 億以下為第四級證券商，其中，第一級證券商應設置資安專責單位及主管。

(2) 要求設置資安長：為型塑證券商重視資安的組織文化，提升對資安議題

之執行能力，進一步要求符合一定條件之證券商應指派副總經理兼任資安長職務，以統籌資安政策推動協調及資源調度。所稱一定條件為資本額 100 億元以上及電子下單比率符合一定條件者；電子下單一定比率指同時符合下列條件： 網際網路下單加計電子式專屬線路下單（DMA）成交金額達公司成交金額 60%。 經紀業務成交金額市占率達全市場 2%。 自然人客戶數達公司客戶數 50%。

2、提升資安人力資源素質：規範資安人員每年應接受 15 小時以上之資安專業課程訓練或職能訓練，其他使用資訊系統之從業人員，每年亦應至少接受 3 小時以上資訊安全宣導課程。

3、提升業者資安防護能力：要求證券商每年度應將前一年度資訊安全整體執行情形提報董事會，以提升公司高層人員對整體資安情況之掌控，另明定證券商公會應訂定資訊安全自律規範，並應配合資訊安全現況定期檢討修正，以利證券商遵循。

（三）證券商內部控制制度標準規範（電腦作業與資訊提供部分）暨建立證券商資通安全檢查機制

為使證券商訂定期內部控制制度有所依循，證交所訂定「證券商內部控制制度標準規範」以供業者參考，另證交所為查核證券商是否有落實相關內控措施，依前開標準規範擇要訂定「建立證券商資通安全檢查機制」，規範證券商辦理資安之內部控制及稽核標準，相關內容分為 14 大主題，涵蓋管理制度、硬體環境、系統作業、網路安全、營運持續及新興科技應用等面向，另考量證券商規模大小不一，爰證交所亦訂定證券商分級防護應辦事項，亦比照證期內控處理準則將證券商分為四級，考量具體執行措施眾多，本節謹歸納相關重點如下：

1、管理制度面：公司應制訂資訊安全政策，並出具資安風險評估報告，至少每年評估一次。另公司應配置適當人力資源及設備負責資訊安全制度之規劃、安排相關教育訓練、明確部門職責區分等，相關人員應依相關法令課予機密維護責任，並設置電腦稽核人員，定期辦理資訊安全查核作業。

2、硬體環境面：公司資訊資產應列有清冊並加以維護。並就實體與環境安全規定，電腦機房應有門禁管制、應配備防災設施、電源供應系統應含不斷

電設備及發電機等。另針對主機共置服務（Co -Location）規定，設備等資產進出主機共置機房應進行申請，並配合清點及留存紀錄、配合定期盤點主機共置機房機櫃內主機與網路設備、及公司放置於主機共置機房之軟體、硬體設備應依遵循相關資安規範等。

3、系統作業面：公司應對資訊系統分級，至少區分核心與非核心系統，另應有使用者權限管理、密碼管理、及資料輸出入管理等，針對系統開發及維護，公司應至少每半年一次辦理資訊系統弱點掃描作業，另就系統委外開發，公司簽訂之契約內容應含資訊安全協定，及對委外廠商資安稽核權等條款，亦應有相關程式原始碼安全規範，此外，因應行動 APP 普及，內控應有行動應用程式安全管理相關規範。

4、網路安全面：公司應定期評估自身網路系統安全，定期或適時修補網路運作環境及作業系統之安全漏洞，網路應依用途區分為 DMZ、營運環境、測試環境及其他環境，並有適當區隔機制，另公司應建立遠端連線管理辦法，對使用外部網路遠端連線至公司內部作業進行控管。有關防火牆管理部分，公司應建立防火牆，進出紀錄及其備份應至少保存三年。有關網路傳輸及連線安全管理部分，公司應每日針對核心系統之帳號登入失敗紀錄，另公司應於投資人網路下單登入時採多因子認證，此外尚有憑證管理、電腦病毒及惡意軟體之防範、網際網路下單服務品質相關標準、滲透測試及資安健診、電腦系統及作業安全管理等多項措施。

5、營運持續面：公司除應評估與交易相關之核心系統可容忍中斷時間外，應訂定故障復原程序，包括電腦設備、通訊設備、電力系統、資料庫、電腦作業系統等備援及回復計畫，另須訂定營運持續計畫（含起動條件、參與人員、緊急程序、備援程序、維護時間表、教育訓練、職責說明、往來外單位之應變規劃及合約適當性等）及其必要之維護，並擬訂關鍵性業務及其衝擊影響分析，並定期辦理業務持續運作演練，以確保公司營運不中斷之能力。

6、新興科技應用面：因應數位科技發展，針對雲端服務、社群媒體、行動裝置、及物聯網之使用訂有相關之內控措施。

（四）證券商公會資安自律規範

因應金融科技與新興資訊科技發展等資安防護需求，證券商公會就目前資訊科技發展所面臨之新興資安議題，定期檢討修訂資安自律規範，內容包括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、物聯網設備安全控管、網路釣魚防範等。並研議將電子式交易身分驗證安全控管，及深度偽造防範安全控管納入該自律規範。嗣配合金管會金融資安行動方案政策，將研議擴大修訂證券商公會資安自律規範之範圍，除現有新興科技資通安全管控外，將納入資訊系統安全防護、網路安全防護、供應鏈風險管理、金融作業韌性等管理措施，期使資安自律規範更為完備。

（五）證券商因應嚴重特殊傳染性肺炎（COVID-19）事件申請居家辦公指引

因應新冠肺炎疫情影響，金管會於 2020 年 4 月 20 日分別核定證交所等相關周邊單位訂定「證券商因應嚴重特殊傳染性肺炎（COVID-19）事件申請居家辦公指引」，規定業者申請居家辦公應有相關資安配套措施，內容包括公司須定時更新虛擬專用網路 VPN 連線和其他遠距連結系統之安控措施、採多因子身分驗證機制、限制僅能由公司員工登入連線，設備操作軌跡應保有完整紀錄、依據員工職掌作業時間訂定可開放連線時段相關規範、教育居家辦公者應對網路風險保持警覺、資料不落地之規範等，證券商並應將居家辦公之各項作業納入內控，並進行內部稽核。

（六）其他

金管會已發布函令規定證券商申請增加業務種類、增加營業項目、設置分支機構及轉投資國內外事業等事項，申請書件應包括資安自評表，相關自評項目包括最近一年發生下列重大資通安全事件，相關資安缺失是否已完成具體改善並經主管機關認可、最近一年經主管機關或證交所等單位查核之資安缺失是否已完成改善、是否遵循相關資安規範並辦理資安查核作業等，以利主管機關將證券商將資安執行情形納入業務准駁之考量。

肆、證券市場資通安全治理

一、定期辦理資安相關會議

金管會證券期貨局定期辦理證券期貨市場資通安全會議，邀集證券期貨市場相關周邊單位，就資本市場之資安現況及國際資安情勢進行檢討分析，精進制度面之管理，

另證交所亦每半年辦理一次證券商資訊主管座談會議，邀集所有證券商之資訊主管，除瞭解業者資安實際執行情形外，亦就實際遇到的資安議題進行討論，同時亦向證券商宣導市場資安重要議題，厚植證券商資安治理之概念。另證交所每半年定期邀集證券周邊單位及相關公會定期召開資安新威脅與資訊科技發展會議，就資安新威脅與資訊科技發展，評估未來資安風險，及檢視現有資安防護機制是否須強化或改善。

二、金融資安資訊分享與分析中心（F-ISAC）

金管會成立「金融資安資訊分享與分析中心（Financial Information Sharing and Analysis Center，F-ISAC）」並委請財金資訊股份有限公司營運，服務對象包含銀行、保險、證券期貨等金融機構，該中心提供會員公司情資研判分析、資安資訊分享、協處資安諮詢與評估、研討會教育訓練及國際交流、資安專題研究分析、協助資安事件應變處理、金融機構資安演練、協助資安規範評估與建議等服務，以利業者事先掌握資安情資，並提升資安預警及分析之量能，營造金融資安聯防體系。

三、定期辦理資安攻防演練

自 2017 年起由證券期貨周邊單位定期辦理國內證券業者 DDoS 攻擊應變演練作業，除驗證流量清洗服務的有效性，並藉此提升業者對應變及通報程序的熟悉度，以掌握對 DDoS 攻擊之防護準備現況，另金管會亦配合行政院國家資通安全會報技術服務中心，辦理金融機構年度 DDoS 攻防演練。

四、證券暨期貨市場電腦緊急應變支援小組（SF-CERT）

為厚植證券期貨相關業者日常資安事件應變處理能量及協調外部資源因應市場重大資安事件，周邊單位及證券期貨相關公會，於 2021 年 11 月 30 日共同成立「證券暨期貨市場電腦緊急應變支援小組（Securities and Futures Computer Emergency Response Team， SF-CERT）」，藉由 SF-CERT 提供業者資安事件處理指引、辦理業者資安事件應變教育訓練及資安事件應變桌面演練、資安事件通報演練、社交工程演練與 DDoS 演練等多樣化之資安演練，致力提高證券期貨市場資安防護能量及業者資安意識與事件應變處理能力。

五、建立證券商資安通報機制及檢查機制，並定期檢討相關資安法規

證券商發生資安事件，應依「證券期貨市場資通安全事件通報應變作業注意事項」進行通報作業，俾利金管會即時有效掌握業者資安事件資訊並為相關因應處理。金管會

亦督導證交所滾動式檢討修訂「證券商內部控制制度標準規範」及「建立證券商資通安全檢查機制」，規範證券商辦理資通安全之內部控制及稽核標準，每年由檢查局、證交所、財團法人中華民國證券櫃檯買賣中心等單位，依相關規定對證券商進行資安外部稽核，並以重大資安事件與證券業相關之案例，參考其發生過程及主要影響內容，列為執行資通安全重要查核項目。

伍、未來精進及強化重點

金管會衡酌市場數位科技發展情形及資安現況，評估證券商之資安監理重點將聚焦於資安政策之落實執行、重大資安事件之影響、及金融檢查發現之重要缺失等項目。經檢視 2021 年度整體證券商資安通報情形，通報數量第一為系統異常相關事件，佔所有事件 53%，次之，則為駭客攻擊事件，佔所有事件 27%，另檢視證交所等周邊單位 2021 年度查核證券商之資安查核，缺失數量最多之前三大類別為網路安全管理缺失，例如未建置「網路下單網頁與程式異動偵測系統」、「防火牆進出紀錄及其備份未依規定至少保存三年」、「未定期或適時修補網路運作環境之安全漏洞」、「網路下單未採多因子驗證方式」等，佔所有缺失數 31%，第二為存取控制類缺失，例如「系統帳號密碼輸入錯誤達三次者未依規定中斷連線」、「尚未能全面使用優質密碼設定，或未能定期 3 個月以內更新相關使用者之密碼」、「未定期審查並檢討久未使用之使用者權限」及「未訂定電腦系統機密性、敏感性之報表列印或瀏覽適當之管制程序」等，佔所有缺失數 28%，第三則為系統開發及維護類缺失，包括「辦理網路下單業務，未依規執行網路系統外部弱點掃瞄作業」、「系統開發及維護之委外作業，與委外廠商簽訂契約內容未包含資安協定與對委外廠商資安稽核權等條款」、「未對弱點掃描所辨識出之潛在系統弱點，評估其風險或安裝修補程式」、「APP 上線前未完成 APP 檢測作業」等，佔所有缺失數 22% 。

綜上分析，考量電子下單普及，有關未來之證券商資安強化重點，將著重於證券商下單系統（含 APP）之穩定，包含系統作業面之各項控制措施及相關備援措施之完善，另亦將強化系統委外開發之供應鏈風險管理；此外，為提升證券商網路安全，防禦駭客攻擊，將強化證券商機敏資料之保護及客戶身分驗證，亦將督導業者建置網路資安防禦設備，例如建置資通安全威脅偵測管理機制、入侵偵測與防禦機制、設置應用程式防火牆等強化措施；至有關因應新冠疫情產生之異地辦公及居家辦公等遠距辦公模式，以及未來運用相關新興科技之營運模式，亦將納入未來資安監理重點。

陸、結語

彭博社 2022 年 6 月 24 日報導[1]，美國財政部為防範潛在網路攻擊，深化跨金融產業間之合作關係，同年 5 月底邀請數家金融機構參加模擬網路攻擊之演練，並於不同場景中測試渠等相互聯繫及協調的能力，美國財政部官員表示，金融業發生資料外洩及遭受資安攻擊事件之排名較其他產業為高，另第三方資訊服務提供者亦存有資安疑慮，面臨越趨複雜的網路環境，金融業必須合作思考及共享情報，以應對資安威脅。

金融市場的穩定，關係國家的經濟安全，在使用數位科技便利服務的同時，亦須審慎對待可能產生的風險，不僅是金融業者應重視資安議題，投資大眾也應培養自身資安風險意識，構建安全之市場環境須仰賴市場所有參與者通力合作，政府亦將指導與協調證券周邊單位超前部署並推行相關資安措施，然資安永遠沒有完美，它有其成本與代價，業者得在資安投入與業務發展之間找到好的平衡，重視安全的同時，又能不影響效率，主管機關在制定相關法令政策時，也會衡平相關成本效益，並與業者充分溝通，以利業者在使用科技創新時，亦能有效控管資安風險。

1　https://www.bloomberg.com/news/articles/2022-06-24/treasury-s-cyber-war-moves-financial-sector-beyond-shields-up#xj4y7vzkg