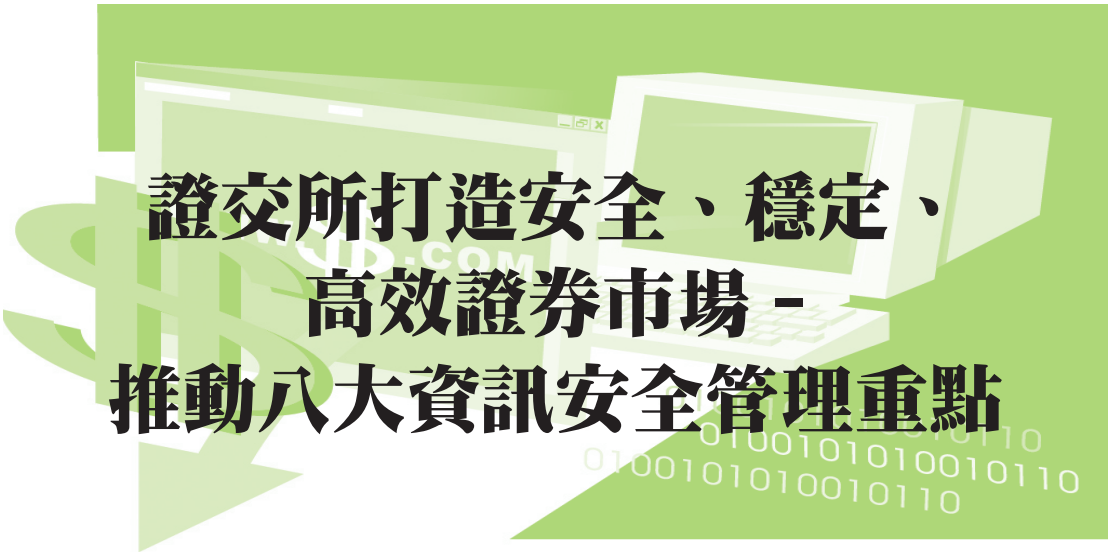
【專題二】



證交所打造安全、穩定、高效證券市場－推動八大資訊安全管理重點

曹華韋（臺灣證券交易所 電腦規劃部專員）

壹、新興資安威脅及挑戰

現今企業的經營面臨無國界化的高度競爭，企業亟思透過資訊科技的應用來強化組織的競爭力、創新能力及風險控管能力，以提升整體營運效率。資訊科技的應用已成為企業營運的骨幹，如何有效的管理資通安全對所有的企業來說，已經不是一個 “nice to have” 的管理議題，而是一個 “must to have” 的核心議題。

近年來，因為資訊科技的演進、全球化的競爭及新興科技應用的推出，導致資通安全管理的挑戰愈來越高。以金融業為例，雲端運算、社群媒體、行動化裝置、新創加值業務（如：APP 服務、第三方支付等），甚至進階持續性滲透攻擊（Advanced Persistent Threat, APT）等資安攻擊手法的演變議題，都是金融業未來必須面對及妥善因應的機會、風險及挑戰。

英國標準協會（British Standards Institution, BSI）與企業持續營運協會（Business Continuity Institute, BCI）在 2014 年所進行的調查中（如圖表 1），歸納出全球各個地域中影響到企業營運的關鍵威脅（以白色標示）及未來的威脅發展趨勢（以黃色標示）。從分析中可以發現影響到企業營運的關鍵威脅大多與資通安全議題脫離不了關係（如：非預期的資訊與通信服務中斷、網路攻擊、資料外洩等）。

中華民國一〇四年三月十六日出版

圖表 1　2014 年 BSI 與 BCI 調查報告：影響企業營運的關鍵威脅及未來威脅發展趨勢

依據世界交易所聯合會（World Federation of Exchanges, WFE）與國際證券管理機構組織（International Organization of Securities Commissions, IOSCO）於 2013 年 7 月 16 日發布之證券市場網路犯罪調查報告（Cyber-crime, securities markets and systemic risk）中，指出全球有 53% 的證券交易所在過去一年曾遭受網路攻擊，並有 89% 的交易所認為網路犯罪可能對證券市場造成整體性的影響。

貳、證交所推動的資安管理重點

證交所於 2015 年 1 月 22 日接受行政院張善政副院長頒發「103 年政府機關 (構) 資通安全稽核績優單位」，表彰證交所於資安發展策略、技術及管理制度等各項資通安全領域的努力成效及全員參與精神。會後張副院長接受媒體訪問時表示，大陸已把臺灣當做網路攻擊的試驗場，府院、外交部、經濟部與國發會，都是大陸網軍最愛攻擊的對象。

圖表 2　行政院張善政副院長（左）頒發證交所李述德董事長（右）「103 年政府機關 (構) 資通安全稽核績優單位」獎

金融業具有指標性、壟斷性、高風險性和效益依賴性等特點，將較一般企業面臨更為嚴峻的資安挑戰，為了因應數位金融 3.0 網路化、行動化、社群化的資安風險，金融業必須要在業務創新、提升競爭力、法規遵循、客戶資料保護、服務品質及資訊安全取得一個平衡點。

證交所為協助整體市場面對營運環境急遽改變的新興資安挑戰，強化資安治理能量，建立前瞻性的資安管理思維，近期推動 8 大資安重點工作，包含：「強化證券期貨市場資通安全聯防及預警機制」、「通過 ISO 27001：2013 年版轉版驗證」、「建立證券期貨市場雲端服務、社群媒體及行動裝置的資安控管原則」、「打造證券期貨雲共享資安防護資源」、「架構共用機敏性資料傳輸機制」、「強化資訊服務供應商風險管理」、「導入進階持續性滲透攻擊（APT）防護機制」、「建置安全、可靠、高效的新資訊中心」等，期能與所有市場參與者共同打造安全、可靠、高效的證券交易環境，達成「流通證券、活絡經濟」之發展願景。

一、強化證券期貨市場資通安全聯防及預警機制

國際證券管理機構組織（IOSCO）於近年來辦理證券市場風險辨識時，不斷強調網路犯罪可能對全球證券市場造成的系統性風險，主因如下：

（一）證券市場高度仰賴資訊科技。

（二）全球各證券市場已複雜且緊密的結合，任何一個證券市場發生問題，皆會連帶影響全球證券市場。

（三）證券市場賴以為生的關鍵因素是對市場交易的信任及信心，若信任及信心因網路犯罪而動搖，將對市場發展及運作造成重大衝擊。

分析近年來網路攻擊趨勢顯示，處於相同產業之業者所遭受的網路犯罪攻擊往往有高度的關聯性，網路犯罪者常鎖定特定產業目標進行攻擊，攻擊手法亦常就產業的特色及產業對於資訊科技的共同應用需求而進行針對性之設計。

因此，WFE 於 2013 年 12 月成立全球交易所網路安全工作小組（Global Exchange Cyber Security Working Group, GLEX）以因應網路犯罪可能對市場造成的系統性風險，藉由此管道讓全球交易所分享彼此之資安資訊，並期望發展產業之安全規範或實務準則，形成全球交易所資安聯防。

我國政府亦針對此一趨勢，於 2009 年 11 月成立政府資安資訊分享與分析中心（Government Information Sharing and Analysis Center, G-ISAC），並鼓勵各目的事業主管機關成立產業資安資訊分享與分析中心（以下簡稱 ISAC），期能透過產業會員間之互信關係，即時分享相關資安情報，達成產業資安早期應變與預警效益。進而由 G-ISAC 橫向交流各領域之資安威脅與訊息，達到情資整合、分享及應用之目的，提升國家資通安全整體應變與防護能力。

對於以網際網路串聯整體產業的數位金融 3.0 時代，證券期貨市場參與者遭受網路犯罪攻擊的可能性亦隨之攀升。為強化整體市場資安防護能量，證交所於 2014 年加入 WFE 全球交易所網路安全工作小組（GLEX），並規劃於 2015 成立我國證券期貨市場資安資訊分享與分析中心（ISAC），藉由蒐集證券期貨市場參與者、國內外交易所、政府機關及其它領域 ISAC 分享之資安資訊，與市場參與者分析及分享資安現況及趨勢，就相關資安議題提出因應措施及防護建議，形成我國證券期貨市場整體資安聯防，有效強化證券期貨市場資通安全。

二、通過 ISO 27001:2013 年版轉版驗證

基於「維護證券市場安全」、「保障投資人權益」與「提昇服務品質」之責任，證交所領先國內外同業積極導入 ISO 9001 品質管理系統（為全球第二家證交所）、ISO 27001 資訊安全管理系統（為全球第一家證交所）、ISO 20000 服務管理系統（為全球第四家證交所）及 BS 10012 個人資料管理系統（為全球第一家證交所）等多項國際管理制度，藉由貫徹國際管理的最佳規範與實務作法，強化公司治理成效，積極回應市場對證交所安全、穩定、效率之要求。

國際標準化組織（International Organization for Standardization, ISO）於 2013 年 10 月的 ISO 年會中，正式推出新版的資訊安全管理系統（Information Security Management System, ISMS）標準 -ISO 27001:2013，這也是 ISO 27001 自從 2005 年正式成為國際標準之後的首次改版。新版 ISO 27001:2013 標準中融入智慧型裝置的管理、供應鏈的委外管理、加密以及系統開發專案管理等新的資安控管要求。

證交所為持續強化資通安全管理及防護水準，自 2014 年 5 月起積極推動新版標準轉版驗證事宜，辦理現況瞭解與差異分析、風險辨識與控管選擇、資通安全管理制度設計與調整、資安管理制度運行與評估等推動階段，於 2014 年 12 月 3 日通過新版 ISO 27001:2013 資訊安全管理系統國際標準驗證，顯示證交所的資安管理制度更往前跨了一步。

三、建立證券期貨市場雲端服務、社群媒體及行動裝置的資安控管原則

以雲端服務、社群媒體及行動裝置等新興科技為媒介拓展之應用服務將成為數位金融 3.0 時代的主流架構，如何確保新興應用服務於開發、部署及營運過程的服務品質及安全，為所有市場參與者皆需面對的重要課題。

為強化證券期貨市場新興科技之風險管控能力，減少個別業者重複投入相關議題之研究成本，金管會證期局於 2013 年 9 月責成證交所邀集期交所、櫃買中心、集保結算所、證券商公會、期貨商公會及投信投顧公會，共同擬定「證券期貨市場相關公會雲端運算、社群媒體、行動裝置資通安全管控指引」，並於 2014 年 8 月由證券商公會函知會員公司參酌，供相關業者衡諸規模大小及業務屬性適度採行之。

為瞭解證券商 / 期貨商相關新興科技的使用現況，協助業者妥適使用管控指引，證交所、櫃買中心及期交所規劃於 2015 年度辦理管控指引宣導及訪視作業，期能藉此協助證券期貨市場有效控管相關新興科技之應用風險。

四、打造證券期貨雲共享資安防護資源

雲端服務為數位金融 3.0 時代的發展重心，現已逐步運用於證券期貨市場，惟金融業所面臨之資安威脅及法令法規要求有別於一般產業，現行雲端服務業者提供之雲端服務環境難以滿足市場參與者之資安防護需求，國內尚無以證券期貨市場參與者為主軸設計之產業社群雲，市場參與者對於雲端服務之資通安全仍存有疑慮。此外，在面臨新型態的網路攻擊時，市場參與者亦難以在短期內投入足夠的資源即時因應資安威脅，市場對建立專屬於證券期貨市場之產業社群雲存有期待。

信任是發展雲端服務的第一要素，證交所為主管機關發展市場暨保障投資之延伸，備受市場參與者信賴，且於資訊系統營運持續及資通安全管理領域有豐富的經驗，皆為

證交所推展雲端服務之有利條件。

行政院於 2010 年起將促進雲端產業發展及加強雲端服務應用列為重要政策，證交所積極響應政府推動促進雲端產業之發展及加強雲端服務之應用政策，與雲端服務業者 - 中華電信公司合作，共同打造符合證券期貨市場產業特性之「證券期貨雲」，除逐步推出法說會影音檔案上傳暨瀏覽雲端服務、證券商下單備用競價雲端服務、逐筆交易體驗雲服務平台及證券期貨資料雲服務平台等多項雲端應用服務外，亦規劃與市場參與者共享防火牆（Firewall）、網頁應用程式防火牆（Web Application Firewall, WAF）、入侵防禦系統（ntrusion Prevention System, IPS）…等資安防護資源，可減少個別公司重複投資及資訊科技維運負擔，協助市場參與者快速應用雲端服務，提升營運效率及服務品質，使市場參與者可專注於創新應用服務的發展。

五、架構共用機敏性資料傳輸機制

於數位金融 3.0 時代的資訊作業環境中，市場參與者間透過網際網路串聯整體產業，市場參與者間存在大量資料傳輸及資料交換需求，惟現行之資料交換之方式不一，針對機敏性資料保護之傳輸保護機制亦有所差異，如何更安全、有效的進行機密及敏感性資料傳輸是推廣數位金融 3.0 的重要課題。

證交所規劃於 2015 年架構證券期貨產業共用之機敏性資料傳輸平台，藉由電子憑證的簽驗章機制，強化資料傳輸及交換過程中之資料加密、身分辨識及不可否認性等機制，提供市場參與者更安全可靠之資料傳輸交換管道。

本傳輸平台初期將邀請證券期貨周邊單位參與試行，並規劃於後續逐步推廣至所有市場參與者。平台規劃採用電子憑證簽驗章機制，使機敏資料之傳遞達到寄件者與收件者間高安全性的端點加密防護，藉由憑證對寄件者之傳輸資料進行簽章，收件者可透過驗章作業確保資料之完整性，並藉此驗證寄件者身分之有效性，滿足身分識別及不可否認性之需求。

六、強化資訊服務供應商風險管理

近年來發生許多重大的供應商資安事件與議題，凸顯出供應商資訊安全管理的重要性，如：

- 是方電訊因電力中斷導致全臺九成對外海底電纜網路服務被迫中斷超過 12 個小時；
- 提供資訊科技服務的 Unisys 公司調查 599 名來自 13 個國家從事石油、瓦斯、能源與製造業等公用服務事業的資安高層，有 67% 的受訪者表示他們的公司在最近 12 月至少發生過一次資安意外；

●美國第二大折扣連鎖商店 Target 遭駭客入侵，造成 1 億多筆客戶資料外洩，起因是一封夾帶惡意程式的電子郵件，第一個受到感染的對象是 Target 的冷藏系統服務供應商；

●南韓遭到大規模病毒攻擊，多家銀行、保險公司、電視台及電信網路業者的內部電腦與網路系統因此癱瘓，這些單位使用同一家防毒軟體供應商的服務，駭客先入侵防毒軟體供應商，再利用病毒碼更新程式派送惡意碼到受害單位；

●微軟發表 Windows 例行性系統升級後，用戶反應當機與顯示異常等問題，微軟承認更新套件存在問題；

●聯想集團完成對美國 IBM 86 伺服器部門的收購，過去由於資安考量，聯想集團一直被排除在臺灣政府供應商名單外，但是隨著此一收購行動，聯想已經成為臺灣伺服器供應商的亞軍；

國際管理系統標準的發展，亦呈現就供應商關係管理日趨重視的趨勢，ISO 組織除了在新版 ISO 27001:2013 資訊安全管理系統標準中強調供應商管理的重要性（供應商管理成為獨立的控制領域，亦新增了兩項供應商相關的控制措施），更於近年來陸續推出 ISO 27036 供應商關係資訊安全系列標準，包括驗證標準（Part I）、參考指引（Part II）、資訊與通信科技（Information and Communication Technology, ICT）供應鏈安全指引（Part III），以及即將推出的雲端服務安全指引（Part IV）。

供應商的多樣性和眾多 ICT 產品的複雜性使得 ICT 供應鏈風險尤其具有挑戰性，但並非不可克服，組織在管理上的挑戰有兩個，一個是有效辨識出可能的風險，另一方面是有效管理辨識出來的風險。證交所依 ISO 27001:2013 資訊安全管理系統要求，強化供應商及其供應鏈之風險辨識、評估及管理，由供應商關係生命週期的角度來辨識面臨的風險，進而幫助組織有效管理供應商關係產生的風險。

此外，針對供應商的實地稽核作業亦是證交所強化供應商服務的利器。證交所除於各式合約中保留委外稽核權外，亦於 2013 年起，實地至各重要供應商辦理「受委託機關個人資料管理」、「資訊服務委外對受託單位」稽核作業（未列為實地訪查之廠商則要求填具「自我評估表」），並將稽核中發現之重要及常見缺失事項，供其他相關供應商參考。上述作法，除可協助證交所有效掌握供應商之資安風險，亦對於提升整體供應商之安全及服務水準有顯著之成效。

七、導入進階持續性滲透攻擊（APT）防護機制

隨著資安防護機制的演進及使用者面對惡意攻擊經驗的累積，迫使駭客的攻擊手法由傳統未針對特定對象的攻擊，逐漸發展出結合針對性、複雜性及持續性等特性的攻

擊手法，以穿透企業築起的資安防護高牆，這類攻擊手法被稱為「進階持續性滲透攻擊（Advanced Persistent Threat, APT）」。

APT 攻擊較知名的案例可回溯至 2010 年由 Google 揭露的「極光行動」，類似的攻擊手法亦於 2011 年讓 RSA 及 SONY 付出慘痛的代價。2013 年 3 月南韓多家銀行、保險公司、電視台及電信網路業者遭受大規模 APT 攻擊，導致相關服務嚴重癱瘓。此事件引起國內政府機關、金融業及資安業者的高度重視，如何降低 APT 攻擊的風險成為國內外資安防護的主要研究課題之一。

Gartner 於 2013 年出版之「Five Styles of Advanced Threat Defense Framework」報告中，對於如何著手強化 APT 的防護機制提供相當完善的建議。Gartner 在報告中指出，對於惡意檔案或執行程式的偵測，不能依賴傳統比對防毒資料庫的方式，而要分析檔案的行為，才能有效地偵測利用零時差漏洞及針對特定攻擊目標所撰寫的惡意程式。對於防護機制的架構方式，Gartner 則建議需要由「事前／中偵測」及「事後鑑識」2 種類型中，各選擇 1 種方式進行防禦，才能兼顧偵測 APT 利用零時差漏洞的入侵行為，及鑑識 APT 於組織內部進行的滲透行為。

證交所參考 Gartner 報告規劃 APT 防護機制的部署方式，分別於電子郵件閘道（Email Gateway）、網路閘道（Network Gateway）及個人電腦（Endpoint）端建置相對應之 APT 防護機制，搭配沙箱檢測 (Sandbox) 與逆向工程（Reversed Engineering）等不同之 APT 防護技術及產品形成資安聯防，並將相關事件紀錄導入由證交所自建之資安監控中心（Security Operation Center, SOC）即時監控、分析及處理各種層出不窮的資安威脅。

APT 主要防護技術說明

APT 防護機制以沙箱檢測技術為主流技術，主因為可於虛擬出的電腦環境觀察及記錄程式是否存在惡意行為，於受隔離的環境中進行模擬及檢測可避免惡意程式感染其他電腦，此類技術在偵測、分析及記錄惡意程式行為等方面皆有良好的效果。

除了沙箱檢測技術，市場上亦發展出有別於沙箱檢測技術的逆向工程技術，該技術主要是將各種惡意行為的程式碼片段，以不同的方式摻入比對引擎中，藉以檢測某個文件檔案是否帶有惡意程式碼。與一般防毒軟體較為不同的是，這技術比對的並非整個檔案，而是更零碎的程式代碼，且主要鎖定文件類型檔案（如：word 或 pdf 檔）。

依據交通大學吳政穎及林盈達教授的研究測試[1] 中顯示，設計良好之 APT 防護產品，無論其採用沙箱檢測技術或逆向工程技術，對於 APT 攻擊的樣本皆可達到 8 成以

1　吳政穎與林盈達（2013）。APT 與偵測方法之分類與分析。

上之高偵測率。

八、建置安全、可靠、高效的新資訊中心

國內首座採用採用隔震工法進行耐震設計的資訊中心，即將於明 (2016) 年第 1 季完工啟用。這是證交所朝強化證券市場資訊基礎建設，建置國際規格資訊中心之策略目標邁出重要的一大步，也同時為證券市場高安全、高效能及高可靠的證券交易服務，提供最佳的保證。

由於證交所肩負證券市場正常運作之重任，職司證券交易的電腦機房未來將遷移至新建的資訊中心，故於設計之初即考量加強建物耐震能力，使建物不因地震發生導致結構損壞，影響證券交易正常運作，故證交所新建的資訊中心建築結構採用隔震工法進行耐震設計，建物設計具備抵抗七級以上強烈地震之耐震能力。此外，為因應節能減碳政策及符合國際趨勢潮流，資訊中心之建築環境規劃設計將以符合綠建築銀級標章認可之標準，建置省能源、省資源、低污染之建築物，為證券市場提供高安全、高可靠及高效能的證券交易服務。

參、結語

「人人資安、事事資安、時時資安」是董事長李述德上任後強調的資安理念，亦是證交所資安治理長期努力的目標。資通安全已是企業日常維運必須注意的議題，不論是從遵循法令法規、主管機關要求、客戶期望或是資訊科技的變革等面向，未來對資通安全治理的要求一定會愈趨嚴謹，企業經營必須正視相關資通安全的威脅及挑戰，證券交易所的資安治理，牽涉證券市場的順利運作，更是應予重視。

證交所的資通安全發展策略，將秉持「流通證券、活絡經濟」的願景，「企業籌資更便捷、大眾投資更穩當」的任務，配合業務發展的需要，適時運用雲端化、網路化、社群化及行動化的服務，並在安全無虞的條件下，提供更優質電腦應用與資訊服務，期以提升整體證券市場的競爭力。

～ 信用交易應循合法管道 ～

投資人從事信用交易應透過主管機關許可之合法業者，避免與非法從事丙種墊款之不法業者往來，以免損及自身權益。