〈轉載自清流雙月刊 106 年 7 月號〉

共構金融資安聯防中心　打造高 CP 值防護網

德明財經科技大學行銷管理系副教授 許建隆

金融機構因業務特性與經濟發展及社會安定緊密相連，在 2015 年行政院資安辦公室公告之「政府機關（構）資通安全責任等級分級作業規定」中，係歸類為 A 級單位（資安責任最高等級），並且定義為關鍵資訊基礎設施，相信在《資安管理法》推行後，公、民營行庫之核心系統仍將被列為關鍵資訊基礎設施，為因應此一趨勢，金融業資安從業人員宜儘早進行相關因應準備。

金融業依法架構資通安全維護計畫

根據《資安管理法》草案第 17 條要求，非公務機關應訂定通報及應變機制，並於發現資通安全事件時應向中央目的事業主管機關通報。目前，由金管會主導規劃推動金融資安中心 F-ISAC 預計於 2017 年第 2 季成立，可預見 F-ISAC 將成為各資安因應金融機構對主管機關通報資安事故或交換資安情資的平台。

前述法規條文與主管單位的動向勢將增加金融業資安從業人員的責任與工作，但若能有效、快速地交換威脅情資，也確實有可能在第一時間讓各金融業者快速應變最新的資安威脅與攻擊，有效避免或降低新攻擊手法所造成的實質或商譽損失。

在《資安管理法》(草案)中，要求公務機關與非公務機關須訂定、修正與實施資通安全維護計畫，也要求主管機關提供範本或施行辦法等資訊供業者參考。但在此之前，公務機關與非公務機關仍可先進行相關準備，檢視是否有不足或未涵蓋之處。首先，可從盤點目前的資安軟硬體設備的投資、資安服務的採購與實質效益、採用的資安制度標準以及相關流程作業，並參照近年的資安風險威脅，檢視現行資安防護投資是否有不足或尚需補強深化之處，更重要的是避免各項資安投資流於僅有單點防護效果，宜透過作業流程將資安防護作業由點連成線，由線構成面，達到整體縱深防禦的資安防護。

資通安全維運作業的 3 大環節

為避免流程的設計僅是應付內部與外部稽核的查核活

動、流於形式，建議金融業者可從「預警與強化作業」、「資安監控與通報作業」，以及「資安事故與情資應變作業」等 3 個相關聯的資安維運作業來檢視與調整現行作業流程。

從 2016 年上半年孟加拉中央銀行的環球銀行金融電信協會（SWIFT）金融電信網路遭駭客入侵跨國盜轉帳案例來看。當金融業者收到此同業之威脅情資時，負責情資管理的資安人員將視情資等級進行內部通報，並針對可能受影響的工作站或主機，擬定對策，呈報決策主管，進行資安情資應變作業，或採行風險降低對策，例如限制工作站對 Internet 的直接存取、建立工作站專用機上的程式白名單管控機制，或加強對可能受影響之工作站電腦上的異常訊息與網路封包之監控通報等。

資安維運人員需要針對預警情資進行篩選、通報管理階層、盤點對應的資訊系統、判斷可能的影響，並擬定適當應變對策方案，快速取得決策階層同意後，投入資源進行對策所需的應變，並在資安情資應變完成後，重新檢視該個案應變過程，並思考是否可回饋到例常的資安強化作業。例如透過年度資安評估作業，檢查防火牆或代理伺服

器（Proxy）是否有依照規劃對此類相關工作站正確設定對 Internet 的存取管控，避免該等工作站遭植入後門程式時傳送內部機敏資訊到駭客的中繼站；並因應該規劃設計資安監控規則，以監控該類工作站的網路連線活動是否有違反防火牆或代理伺服器（Proxy）對 Internet 的存取管控規則；再根據此規則確認資安事故通報與該類資安事故之應變作業程序。

如此從「預警與強化作業」、「資安監控與通報作業」與「資安事故與情資應變」等活動循環落實資安維運作業，累積的資安經驗有助於提升金融業者面對相關資安情資的應變活動。

金融資安聯防中心功能何在？

若建立金融資安聯防中心，除了提供資安監控服務，宜提供以下功能，以強化其對於金融業者之效益：

1、提供針對性之資安弱點情資通報。未來金融產業界之資安資訊分享與分析中心（F-ISAC）雖然提供資安情資，但尚未規劃針對個別會員的需求在通報前事先過濾篩選情資，故預期其會員未來所收到之情資數量眾多，而與

業者切身相關者寡少，業者自身之資安維運人員將需要花費許多工時用以過濾情資。因此，金融資安聯防中心若能對個別業者提供針對性之資安情資，並予以分類及建議風險因應之優先等級，將可節省業者相關人力工時，並提升因應作業之時效性。

2、提供事故處理經驗庫。金融業者間具有競爭關係，對於所遭受之資安攻擊事件與應變處理方法等詳情可能不宜與同業共享，但金融業者同為資安攻擊之熱門標的，各業者所遭遇之攻擊手法相似性高。因此，金融資安聯防中心若能將會員遭遇之攻擊事件與應變處理經驗予以匿名化處理，再提供給其他會員參考，將有助於提升個別業者事故因應之時效性，降低損失，並供部署強化措施之參考。

3、與國際資安組織接軌。金融業者拓展全球性業務時將面對國際化之資安防護要求，可能需要與多個國際性之資安資訊分享與分析中心介接，以提供自身之資安情資，或接收國際組織之資安情資。若資安聯防中心具備與國際ISAC 之介接能力，將可免除金融業者自行開發與維運介接介面之負擔，順利與國際接軌。

全面升級資安防護，接軌國際

資安威脅、資安情資攻擊手法瞬息萬變，駭人的入侵新聞案例更令從業人員面對巨大的挑戰，《資安管理法》或許會更增加資安從業人員的責任與負擔，更直接增加企業營運成本，資安從業人員或許可藉此爭取更多的資源投入，重新檢視目前配置的資安軟硬體設備人力與組織架構，將現有投入或不足之處補強，由單點防護透過流程作業串聯成線，透過點線相連形成完整的資安防護面，最後構成整體防禦縱深，確實落實於資安維護維運計畫與作業。為使金融業者投入的資安投資更具效益，宜考量建立金融資安聯防中心，以收提升資安防護時效、降低損失，以及順利與國際接軌之綜效。