【專題三】

淺談資通訊設備供應鏈安全

戴孝如（臺灣集中保管結算所高級專員）

壹、前言

傳統的供應鏈與供應鏈管理多著重在生產與供給，從採購、製造、配送到銷售等一連串的營業活動，似與證券期貨業者的營業活動完全不搭，換個角度與層次，以終為始，採終局思維，逆向來看，證券期貨業者是提供投資人買賣股票期貨的平台，也就是產製「資訊服務」商品，資訊服務之所以能產生，涉及了資訊設備、應用系統、網路通訊等，並非自家公司就能獨立完成，需結合資訊軟硬體設備供應商與網路通訊業者等，形成資通訊設備供應鏈。

現今駭客的精進，其專業程度不僅只限於技術而已，已轉型為產業分工，構成產業鏈，並且各有專攻領域，打的是團隊戰，而且是有規劃有效益的進行攻擊，了解金融證券期貨業者非常重視資通安全，均建置有資安設備，與建立防護機制，直接對其進行攻擊，須花費較高的精力與較多的天數，基於成本效益分析，多數不會採用直接攻擊金融證券期貨業者系統的方式，改由曲線路徑，反而比直線路徑更能到達目的地，轉而選擇由其投資人或供應商端著手。

2020 年 12 月網路安全公司 FireEye 揭露一個很可能是國家級駭客所為的

「SolarWinds 資安攻擊事件」，甚至推測有多個駭客團體參與其中，被外國媒體比喻為近年來最大的資安攻擊事件，牽連甚廣，美國有多個政府組織、資安業者與大型科技公司都受影響。

SolarWinds 是一家軟體公司，以發展企業管理網路、系統和資訊基礎設施的資源監控與管理聞名，從美國、歐洲，一直到亞洲的印度、中國大陸、日本與台灣都有採用它們旗下產品。「SolarWinds 資安攻擊事件」為駭客將惡意程式植入其開發之 Orion 網路管理監控產品，受感染的檔案隨著產品更新一併派送到各用戶端，導致企業用戶可能因為安裝該程式而受到損害，連發現此攻擊事件的 FireEye 都表明因此遭駭，導致該公司紅隊測試的工具外洩。

後續由 SolarWinds 官方陸續公布事件入侵時間序，發現早在 2019 年 9 月可能就開始受到有計畫的入侵，從入侵單一公司或產品最後導致超過 18,000 個企業客戶受到感染，整個影響過程透過信任圈一路擴大，被認定為是重大的「供應鏈攻擊」。雖然這起事件對臺灣影響小，但其嚴重程度，引起全球對網路供應鏈攻擊的重視，有許多值得我們深切思考與警惕之處。

COVID-19 造成的大規模封城、停班與停課，但藉由網路，搭起人與人、企業與企業的聯繫橋梁，在家裡不出門依然能工作與學習，也因為現在已是網網相通的世界，所以任何一企業的資通安全防線，都有可能因第三方的因素，遭突破而受到攻擊，經由過往的經驗記取教訓，由別人付出的學費中獲得收穫，改善、強化與精進自身的資通訊設備供應鏈管理與監督作業，以為因應類似事件之再發生。

貳、掌控供應鏈安全

近幾年相繼發生重大供應鏈資安事件，各國政府陸續研擬制定供應鏈安全政策，要求關鍵產業針對其供應鏈進行資通安全風險管理，透由管理達到事前防範，以降低風險。供應商的市場口碑僅能作為邀商參考，拋開對原有觀點，從零切入，對其資通安全機制進行了解，確認風險後，再串起鏈結，納入信任圈，以避免造成資通安全防線的破口。駭客戰力都提升到團體戰，信任圈內的供應鏈也應相互合作的訊息分享與即時通報，共同面對資安威脅，以期於事件發生時有效因應，防止可能造成的損害與控制影響範圍。

一、管理政策

2015 年美國國家標準暨技術研究院（National Institute of Standards and Technology，NIST）發布「SP 800-161」文件中，提出「Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations」（網路安全供應鏈風險管理指南），並於 2022 年 5 月釋出新版文件：「SP 800-161r1」，目的是幫助企業獲取與使用技術產品與服務時，保護自身的安全，指南敘明供應鏈可能產生的風險，企業與供應鏈之間的關係，協助企業辨識、評估與應對供應鏈所帶來的網路風險，可作為資通訊設備供應鏈安全作業的重要參考。

2017 年 9 月歐盟所提出之「Cybersecurity Act」（歐盟網路安全法），已於 2019 年 6 月 27 日正式生效，重新強化歐盟網路安全機構（European Union Agency for Cybersecurity， ENISA）的地位與資源，建立資訊、通訊相關產品、服務、流程的歐盟網路安全認證框架（European cybersecurity certification framework），並預期 2023 年將有許多資通訊產品（如：5G 設備）將被列入強制認證項目。

我國政府推動「資安即國安」的國家戰略，於 2018 年公布之「資通安全管理法」與 6 項子法。其中資通安全管理法第九條：公務機關或特定非公務機關，於本法適用範圍內，委外辦理資通系統之建置、維運或資通服務之提供，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。以及「資通安全管理法施行細則」第四條，規範了各機關依資通安全法第九條規定委外辦理資通系統之建置、維運或資通服務之提供，選任及監督受託者時的九項應注意事項。

為因應近期資安事件，多數起源於供應商，2022 年我國政府再公告「資通系統籌獲各階段資安強化措施」，依強化措施中所提依據為「資通安全管理法」第九條，措施所適用對象也就涵蓋受資通安全管理法規範之機構。以及公告「金融機構資訊委外之資安應注意事項」，建議銀行、保險、證券期貨、投信投顧各業別之公會，參考納入資訊作業委外資安相關自律規範之訂定。

綜上法令法規公告顯示，政府對資通訊設備供應鏈安全有著高度關切與強力要求，企業應加強對供應商的資通安全要求，與列為風險評估項目，亦有助於避免發生供應鏈攻擊或由供應商造成的資安事件。

二、Zero Trust 零信任

「Zero Trust 」係為在確認可信之前，沒有任何連線、使用者或資產可以信任，是一套方法，所以除了運用在資安網路架構上，也可套用於資通訊設備供應鏈，不只是應用系統開發的委託業務，也包含軟硬體設備的採購，面對不熟悉與未知的供應商，都需警戒對待，了解其資通安全認知、防護機制與相關作為。

為何需了解供應商的資通安全相關作為？系統可粗分為架構、設計、開發、部署等階段，而各階段都有可能遭有心人利用，透由軟體、韌體交付、派送，送達客戶端，也就是我方，所以知悉瞭解供應商日常的資通安全各項相關作業是有其必要性，確認委託業務與該供應商的風險為我方可接受範圍後，再將供應商納入信任圈。

（一）供應商風險評估管理

委託前對供應商進行評估，了解供應商的資通安全各項作業，評定會對我方帶來何種的風險，委託後持續監控與定期評估供應商的資通安全作為，用以確認原評估風險是否有所變化，倘風險提高時，才能及時研擬風險管控措施以為因應。

評估內容包含供應商之專業能力、維運能力、經驗實績、資通安全防護機制與供應商人員的資安意識，或選擇委託業務範圍之資通安全管理措施通過第三方驗證之廠商，也需考量供應商是否曾遭資安攻擊、發生資安事件，相關後續的改善強化措施與執行效益等，涉及雲端服務時，還需要求供應商提供雲端運算資通安全管理措施。

持續監控與定期評估執行方式，除經常使用的實地稽核抽查作業外，還可包含項目有：要求供應商定期提交資通安全作業自我檢核報告、弱點掃描結果與漏洞修補報告等，以及對供應商執行滲透測試作業，亦可委由專業機構於暗網蒐集供應商訊息等作為，以確認供應商的風險為我方可接受範圍。

另外供應商與產品的血統、出生地、人力資源等，也是資通訊設備供應鏈安全需要考慮的一環，例如美國對俄羅斯安全產品與中國大陸智能手機都有發布相關禁令，本國對中國大陸的設備與工程師亦有所疑慮，這本是不可忽略的「地緣政治風險」，應將其納入我方核心業務之軟硬體設備與服務採購作業風險評估因素內。

（二）明訂服務水準

製造業、零售業為確保產品有統一穩定的品質，對所採購之原物料或商品都訂有規格標準，為了準時出貨與上架銷售，與供應商之契約，也訂有到貨期限或到貨延遲備援方案，多少對能因應類似 2021 年 3 月蘇伊士運河阻塞事件，運輸中斷造成斷貨危機。同理可證，要維持穩定的資訊服務品質，契約明訂服務水準有其重要性。

為了確保我方對外能持續提供穩定有品質的服務，應與資訊供應商所訂之服務水準內容，對品質的要求僅僅只是基本款，依委託業務的流程、資料流與資通安全基準，規範資通安全項目，如系統可用率、開源軟體、系統安全性證明，及上述（一）供應商風險評估管理中，所提資通安全防護機制、稽核抽查、要求供應商提供弱點掃描結果與漏洞修補報告，適時完成我方發現之資安缺失等納為服務水準要求項目，並且應有是否允許轉讓、分包、下包等要求，以能適時控管第三方供應鏈。

委託業務涉及雲端服務，還要訂定雲端的管理事項與災難復原時限，因為雲服務的實際管理在於雲服務廠商，所以必須確認供應商的管理能力與備援方式，以確保我方權益。

（三）驗收與維運保固

有明確的服務水準就應依其進行驗收，如使用第三方供應鏈或開源軟體，供應商與第三方之契約，服務水準要求應等同我方對供應商之要求；開源軟體後續的版本更新與漏洞修補作業執行程序與方式等，也應有明確規範。系統安全性證明應要有源碼檢測、弱點掃瞄或滲透測試結果報告等具體證明，而非僅是供應商的一紙承諾書。

維運保固，如可檢視供應商的持續營運計畫（BCP）、異常狀況的應變與復原演練，及備品與人力資源等情形，以確保對系統可用性的維持能力。適時完成我方稽核抽查、執行滲透測試作業，或暗網蒐集所發現之資安缺失事項，以確保資通安全防護機制的有效性。檢視供應商對資安事件的回應機制，以確認其能及時控制損害範圍、恢復正常運作，與通知我方準備因應。

三、建立聯防

2017 年 12 月金融監督管理委員會為提升金融體系資安防護能量，成立「金融資安資訊分享與分析中心（Financial Information Sharing and Analysis Center , F-ISAC）」，服務對象包含銀行、保險、證券期貨、投信投顧等各業別金融機構，提供通報、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、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 9 大服務功能，建構金融資安聯防體系。

臺灣證券交易所、臺灣期貨交易所、財圖法人中華民國證券櫃檯買賣中心、臺灣集中保管結算所等 4 家證期周邊單位，與證券期貨業者相互間的關係，以證券期貨交易的觀點看，形成一資訊服務提供的供應鏈。

2021 年 11 月證券期貨相關機構成立「證券暨期貨市場電腦緊急應變支援小組（Security and Future Computer Emergency Response Team，SF-CERT）」，由臺灣證券交易所、臺灣期貨交易所、財圖法人中華民國證券櫃檯買賣中心、臺灣集中保管結算所，以及相關同業公會所共同合作維運，7*24 小時協助證券期貨業者應變資安事件，及辦理資安演練與訓練。

金融證券期貨業者已建立完整的聯防機制，均能適時取得資安相關訊息，應可於可提供範圍內，將訊息轉通知供應商，或納入後續新契約要求，亦或適時辦理增補契約條款，要求供應商辦理相關資安作業，由小處作聯防，補強供應商的資安機制。

而最簡單的聯防，就是要求供應商當發現異常狀況或疑似資安事件時，應立即通知我方，以提早準備因應。而做到通知這件事，有一項重要、很重要、非常重要，卻不被重視且常被忽略的 " 基本元素 "：「供應商與我方應確保知道如何聯繫對方」，要知道對的聯絡人員與聯絡方式，才能達到有效又有效率的效益通知，所以隨時更新保持正確的聯絡資訊，對異常狀況與資安事件能否及時溝通處理極為重要。

參、結語

以終為始，終局思維，金融證券期貨業者為客戶提供完整、效益與安全的金融交易資訊服務平台，以此為重點，重新釐清對資通訊設備供應鏈安全之要求與相關法令規章，自我確認我方的標準後，著手檢視內部各項做法與程序，及供應商的契約，再依檢視結果評估需增修訂之項目，規劃草擬內容、試行運作，依試行結果調整作業，必要時

與供應商簽訂增補契約條款，以補足資通安全機制項目。

這項作業不算是件小工程，依各企業經營管理層級或主管機關慣性的標準，多數為整體、全面性的檢視，為了提升檢視效益，可採用「由核心向外，逐步進行」，改善提升資通訊設備供應鏈之安全，以期避免發生供應鏈造成之資安事件。