【專題二】

證券商因應遠距工作之資通安全強化措施

劉保鈞（證交所專員）

壹、前言

一場疫情改變了全世界，新型冠狀病毒（COVID-19）對全球的影響，迫使各機構及個人不得不改變工作的模式。由於病毒強大的傳播力，造成龐大的醫療負擔及重大傷病，為緩解病毒對社會的衝擊，衛生福利部疾病管制署（CDC）公布相關指導措施，減少人與人之間的接觸，期能降低群聚感染風險。為此，公司需因應時勢所需，尋找新型態的工作方式，因此遠距工作在疫情肆虐的這幾年，大量被運用在各行各業之中，這種不受地點及時間限制的資訊技術在這個時局下提供了極大的彈性，讓各機構得以在這樣的環境下保持運作。惟遠距工作帶來了優點，同時也伴隨著缺點及風險，如何將相關優點發到極致，把缺點及風險降至最低，是各機構及監理單位所關注的。

近年來企業十分重視資安韌性，藉由導入新的技術及各種演練來強化業者面對異常事件的營運量能，以確保服務品質。為此企業投入了大量的心力在滿足這些目標上，而遠距工作亦為達成前揭目標，一個必要的手段，為此業者使用各種方法，來獲取遠端工作的效益，雖然便捷的技術幫助業者在業務執行上，但也為此帶來資安控管的議題；本文主要探討證券商因應遠距工作之資通安全強化措施，從遠距工作的特性、法規控管及

查核情形，分別由技術面及管理面介紹相關作業，說明相關強化措施及落實監理作業。

貳、遠距工作的特性

一、定義

根據顧能有限公司（Gartner）定義，遠距工作也稱為在家工作（work from home ,WFH）或遠程辦公，是一種靈活的工作安排，允許員工在公司辦公室以外的遠程位置工作。對於可以在異地完成工作的員工，這種安排有助於確保工作與生活的平衡、獲得職業機會或降低通勤成本。對公司的好處包括提高員工滿意度和留職率、提高生產力和節省資源成本。遠距工作安排可以是臨時的或永久的、兼職的或全職的、偶爾的或頻繁的。遠距工作需要管理設備使用、網路安全和性能預期的政策。

根據思科（Cisco）發布《未來安全遠端工作研究報告》（Future Secure Remote Work Report），統計了在 COVID-19 疫情高峰期，各地區辦遠距辦公的情形，發現台灣遠距工作人員與世界其他地區相比數量較少，只有 32%，低於全球平均 40% 及歐洲平均水平 45%。另報告也指出亞太地區的企業組織在實施大規模遠距辦公時，面臨網路資安風險大幅提升；其中，73% 的臺灣企業自新冠肺炎疫情爆發以來，經歷比疫情發生前多了網路資安攻擊或攻擊警報，此比例高於亞太地區平均值 69%，這說明這種新型態的工作模式雖帶來便利，但也讓資安的攻擊與日俱增。

二、優點

（一）強化資安韌性，在發生意外災害或是像現今大型傳染病發生時，可以在辦公室以外之合適地點與時間迅速恢復工作，避免企業因相關意外事件而無法順利提供對外服務，導致業者及客戶的重大損失。

（二）減少能源浪費，對於各產業推動企業永續經營的理念，遠距工作是一個有效降低能源使用及汙染物排放的方式。

三、缺點

（一）工作與休息的分界不明，因為沒有地點的限制，有可能造成內部員工在非上班時間辦理業務，造成人員額外負擔。

（二）資通安全控管上的風險，可透過遠端連線進行存取，對於機敏性資料的控管及人員權限，面臨很大的挑戰。

（三）互動性不足，透過遠端軟體缺乏臨場感，現行的作業需調整流程，始得利於遠距工作的應用。

四、資安風險

（一）使用不安全的網際網路連線至公司，遠距工作的員工如果透過公共網路或不安全的家庭無線網路連線至他們的公司存取文件。這可能導致網路攻擊者得以藉此存取機密和敏感資訊並攔截或竊取資料。

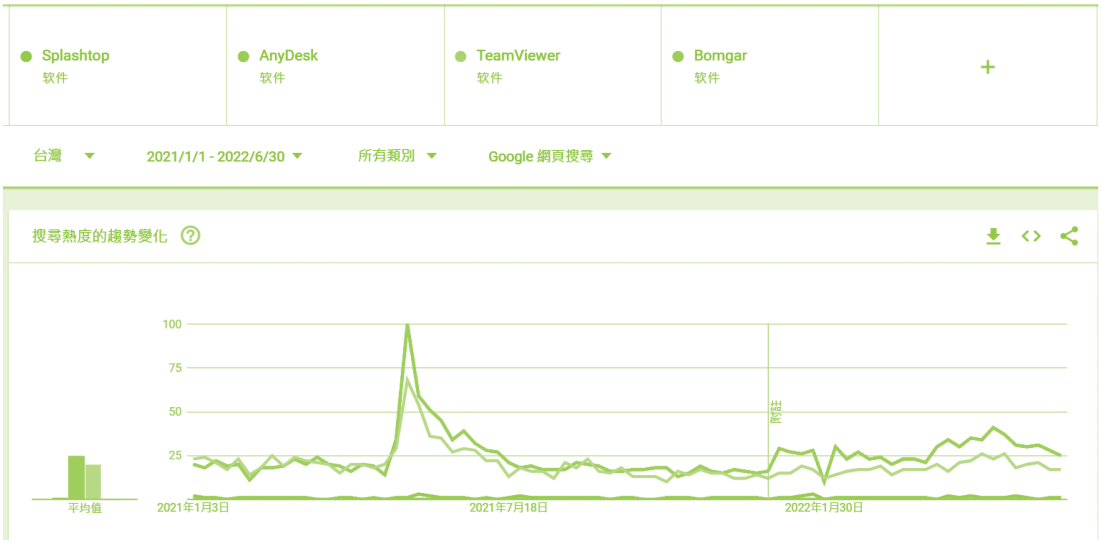
（二）個人電腦工作和個人事務混合使用，許多遠距工作的員工，使用自己的個人電腦進行工作，因此也會將這些設備用於私人用途。這個風險是員工可以將機敏性資料保存在他們的個人電腦上，甚至在沒有任何保護的情況儲存或使用。

（三）弱密碼導致資安漏洞，一些員工為他們的帳號和應用程式選擇了弱密碼或可預測的密碼，這可能會使整個公司的安全面臨風險。例如所有帳號都使用相同密碼的人一旦有部分密碼遭竊取，或網路攻擊者成攻駭進了一個帳戶，他們就可以存取其他相關的帳戶。

（四）網路釣魚和社交工程目標明確，透過遠端連線工作，讓許多員工成為網路釣魚和社交工程的首要目標。網路攻擊者常利用這些電子郵件騙取重要資料；甚至安裝了木馬程式或惡意軟體開啟連線至公司的後門，造成資安破口漏洞。

五、遠距工作之實際運用

（一）透過第三方軟體或微軟遠端桌面功能直接連線操作目的端電腦，現行主流的遠端工作軟體為 Splashtop、Anydesk、Teamviewer、Bomgar，惟本文僅透過 google 搜尋熱度作為使用度之替代指標。根據前揭搜尋結果，發現臺灣目前遠距工作軟體之搜尋熱度多以 Anydesk 為主流，在實務查核上亦有發現相關軟體之運用。



資料來源：google trend

（二）使用虛擬私有網路（virtual private network ,VPN），建立安全連線或網際網路連線至公司員工入口網站（portal）進行登入，完成登入驗證後使用虛擬桌面（virtual desktop infrastracture, VDI）等技術，執行遠距工作。

六、控管措施

（一）連線至公司內部時採用虛擬私有網路，遠端連線至公司內部時採用虛擬私有網路，透過與公司伺服器建立安全的加密通道，避免遭到網路攻擊者攔截資料。

（二）採用多因子及動態密碼管理，身分驗證應採用多因子認證機制，於登入時除了輸入帳號、密碼外，另採用其它因子如與個人顯性資訊無關之隨機數字代碼、令牌（token）、金鑰、生物辨識等其他因子，驗證遠端工作者之身分，以完成遠端登入作業。

（三）最小權限管理原則，遠端工作者帳號登入時應與公司內部權限配置一致，避免讓遠端工作者於公司外部，有機會以過高權限帳號存取公司內部系統。

（四）設置連線跳板機，公司應設置連線管理工作站，監控對公司內部之連線並留存相關操作軌跡，並包含完整回放及即時監控功能。

（五）建立防火牆管制連線存取，設定來源 IP 及開啟必要服務埠（port），以控管連線，避免外部不必要之連線。

（六）工作環境及連線設備實體管控，遠端工作者應審慎評估遠端工作環境，避免於公共場所處理公務作業，使用連線設備如符合員工自攜行動裝置設備（BYOD），應明訂使用限制、設備遺失通報等責任。必要時應對長期遠端工作者辦理遠端工作安全教育宣導。

參、法規控管

為強化遠距工作資安防護，證交所同周邊單位訂有「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」、「證券暨期貨市場各服務事業資通系統安全防護基準參考指引」、「建立證券商資通安全檢查機制」、「內部控制制度標準規範」，作為證券業者辦理遠距工作之參考及依據，就系統面、網路連線面及管理面各面向控管，輔導證券業者強化遠距工作之資安控管。

一、「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」

（一）公司須建立安全的遠距連線機制（如：VPN、VDI）包含：採多因子身分驗證機制（員工帳號密碼、動態密碼、一次性帳密）、加密連線、採最小授權原則、留存完整使用者操作稽核軌跡、監控與警示異常操作行為、執行安全性漏洞更新等安控措施，並教育居家辦公者應對網路風險保持警覺等。

（二）公司須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，並依據員工職掌作業時間訂定可開放連線時段相關規範。

（三）公司須透過防火牆來阻擋惡意或未經授權之連線，並以最小權限原則設定規則及關閉非必要之埠號，並應監控網路流量及異常警告及中斷連線機制。

（四）公司須以最小授權原則，對使用者進行存取系統權限之差異化管理，居家辦公者僅能有執行業務之必要功能權限，關閉非必要之系統功能授權。

（五）電腦設備（含筆記型電腦及平板電腦）應安裝特定資安軟體，控管應用程式存取權限，並關閉電腦上非必要之服務及作業系統權限，進行遠距工作應採技術面手段實現資料不落地機制（採技術面手段禁止傳輸及儲存檔案至居家辦公者電腦設備），降低資訊外流風險。

（六）要求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，留存相關維護紀錄並由權責主管定期覆核。

（七）公司應每年定期檢視並維護防火牆存取控管設定，並留存相關檢視紀錄。

二、「證券暨期貨市場各服務事業資通系統安全防護基準參考指引」

（一）組織應訂定遠端連線管理辦法，建立使用限制、組態需求、連線需求及文件化，對於任一允許之遠端存取類型，均應先取得授權，並留存相關紀錄。

（二）組織應於伺服器端完成資通系統帳號權限登入驗證作業。

（三）組織應監控使用外部網路遠端連線存取組織內部網段之連線。

（四）資通系統應採用連線加密機制。

（五）資通系統遠端存取之來源應為組織已核准之存取控制點。

三、「建立證券商資通安全檢查機制」

（一）通訊與作業管理（CC-17000）項下 (1) 網路安全管理之 e. 公司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（如防火牆、虛擬區域網路、實體隔離等）。

（二）通訊與作業管理（CC-17000）項下 (1) 網路安全管理之 h. 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，留存相關維護紀錄並由權責主管定期覆核。

（三）電腦系統及作業安全管理（CC-17020）之 e. 公司透過網際網路使用管理帳號登入重要系統時，應採用多因子認證機制。

（四）存取控制（CC-18000）項下 (3) 密碼管理之 f.…公司應使用優質密碼設定（長度 6 個字元（含）以上，且具有文數字或符號）並進行管控…

（五）存取控制（CC-18000）項下 (3) 密碼管理之 g. 檢查公司現有之網站、伺服器、網路芳鄰、路由器、交換器、作業系統及資料庫等軟硬體設備應設定使用密碼，且避免使用預設（如 administrator、root、sa）或簡易 （如 1234）之帳號密碼及未設管理者存取權限。

四、其它金融相關業別對於遠端工作控管之簡介

（一）「金融機構電子銀行安控基準」

使用遠端連線進行系統管理作業時，應使用足夠強度之加密通訊協定，並不得將通行碼紀錄於工具軟體內。

（二）「金融機構資通安全防護基準」

1、使用遠端連線進行系統管理作業時，應使用加密通訊協定，並不得將密碼紀錄於工具軟體內。

2、經由網際網路連接至內部網路進行遠距之系統維護管理工作，應遵循下列措施：

(1) 應建立授權機制，依據其申請項目提供必要授權。

(2) 應定義允許可連結之遠端設備，並確保已安裝必要資訊安全防護。

(3) 應加強變更作業之身分認證，於每次登入時得採用照會或二項以上安全設計並取得主管授權，惟緊急故障排除仍須於事後向主管核備。

(4) 應建立監控機制，留存操作紀錄，並由主管或獨立單位定期覆核。

（三）「電子支付業之電子支付機構資訊系統標準及安全控管作業基準辦法」

經由網際網路連接至內部網路進行遠距之系統管理工作，應遵循下列措施：

1、應審查其申請目的、期間、時段、網段、使用設備、目的設備或服務，至少每年一次。

2、應建立授權機制，依據其申請項目提供必要授權，至少每年檢視一次。

3、變更作業應加強身分認證，每次登入可採用照會或二項（含）以上安全設計並取得主管授權。

4、應定義允許可連結之遠端設備，並確保已安裝必要資通安全防護。

5、應建立監控機制，留存操作紀錄，並由主管定期覆核。

（四）「保險業辦理資訊安全防護自律規範」

1、針對營運環境調整、資料傳輸及加密機制、機敏資料防護、稽核軌跡留存、異常行為監控及對外遠端存取設備進行評估及強化，系統及設備如有重大漏洞應立即處理及因應，降低業務運作風險，確保整體保險系統穩定及安全。

2、針對使用之視訊會議系統、VPN 及 VDI 等設備，應訂定相關使用規範並落實各項安全管控作業。

綜上，檢視證券業及相關金融業對於遠距工作連線控管，大致可彙總為以下幾點：

（一）建立加密連線或傳輸加密，以避免機敏資料遭竊取，連線均要求採取加密。

（二）設置防火牆阻擋，確保特定來源之 IP 可連線進行存取。

（三）連線設備之安全控管，對於可連線至公司內部之設備採端點控管，並安裝防毒軟體以強化資安防護。

（四）強化驗證機制採用多因子驗證或動態密碼方式登入，確保正確識別登入人員身份。

（五）要求採用優質密碼至少採文數字混合之六個字元密碼，避免密碼遭破解，並要求至少每三個月進行密碼變更。

（六）留存連線軌跡備查，確保遠距作業得以追溯，釐清權責及落實監控機制。

肆、輔導業者辦理情形

經統計近兩年遠端連線作業相關缺失多為未依公司所訂之規範辦理及未留存相關連線軌跡，彙總如下：

一、缺失項目：

（一）遠端連線維護未進行適當之控管（如：留存連線紀錄、重設其登入之密碼及防火牆規則未控管等）

（二）尚未建立遠端連線管理辦法或未留存、覆核相關維護紀錄。

二、缺失案例說明：

（一）證券業者之資訊系統維護廠商於公司外部透過網際網路，以遠端遙控軟體連線至承辦人員個人電腦，經承辦人員同意後，執行程式變更暨維護作業。惟周邊單位於查核時發現該業者未依該公司所訂遠端連線規範辦理，如使用具管理者權限之應用系統帳號執行程式更新版本暨維護作業且未留存維護作業紀錄

（二）周邊單位對證券業者進行資安查核，檢視業者之遠端連線作業，發現遠端工作人員得透過網際網路以遠端桌面連線（Remote Desktop Protocol）方式連線至伺服器主機，經查該項之防火牆規則，雖有依規定填具「資訊廠商防火牆開通申請書」並限定來源 IP 位址及開放時間，惟未採用多因子認證機制，且未定期覆核外部網路遠端連線至公司內部作業之紀錄。

三、建議措施：

（一）建議證券商應評估遠端遙控軟體之安全性，並透過防火牆或遠端軟體之控管，採限制連線來源 IP 位址及加密方式進行連線，以確保遠端連線之安全。

（二）如委外廠商之人員如因作業需求，需進行系統存取時，應由該公司人員填具申請單代為提出申請，獲核准後始得連線。另限制委外人員遠端連線僅限連線至跳板機，透過跳板機再連線至目的主機進行維護，且連線均由側錄系統錄影以留存相關操作紀錄。

伍、結語

全球爆發新冠肺炎疫情為各個產業帶來了莫大的衝擊，但企業為了能在這樣的艱困的環境中存活下來，運用了許多資訊技術強化公司作業韌性。在後疫情時代，混合型態的工作環境可能會成為主要的趨勢，如何打造一個行動辦公的場所，讓每個員工都能不受地點及時間的影響，是公司未來努力的方向。關於混合工作環境，全球各大企業都在嘗試把這個新的模式融合在現行的企業流程裡面，微軟認為混合工作需要一種新的運營模式和戰略，其中包括靈活的工作政策、包容性的空間設計和創新的技術解決方案。倫敦證券交易集團（London Stock Exchange Group,LSEG）認為他們重視工作的品質，而不是完成工作的地方，在疫情大流行期間的遠距工作經驗顯示這種工作方式的靈活性及有效性；因此混合工作模式讓員工選擇家和辦公室之間分配時間，靈活地工作，同

時無縫連接並保持高效能，讓員工身在何處都能發揮最佳狀態。根據思科研究報告，有 22% 的台灣企業預計未來會有超過一半的員工持續遠距工作，雖然低於亞太區平均值 34%，但仍較疫情前的 14% 高出許多。此外，隨著混合辦公模式成為新趨勢，高達 85% 的台灣企業同意資安在疫情爆發後更顯重要，78% 的台灣企業在疫情期間開始導入資安的解決方案，實際解決資安的漏洞及威脅。

綜上，遠距工作這種新型態的工作方式未來將逐漸為各行各業所採用，企業除了享有科技帶來的便利外，同時也要面對便利所帶來各種隱憂，如何整合這個全新的混合工作模式以達到最大效益，是企業要審慎評估，公司決定實施混合工作模式前應先有良好規劃並定期檢視是否產生新風險；而這一類工作型態對公司監理三道防線也會有一定程度的影響，包含應建立混合工作模式申請作業程序、評估是否限縮得採遠距工作者得從事工作範圍、所在地或國家範圍、強化遠距工作者相關法律責任之認知及要求等，如何透過管理規範及控制措施來確認遠距執行業務對於法令遵循之落實情形，也是監理機關新的挑戰。

參考資料

1. 陳憲昌，「遠距工作之可行性研究」（中山大學企業管理學系，2011 年）。

2. 謝昀澤，「證券業數位轉型的趨勢與挑戰」（臺灣證券交易所 60 週年特刊，2021 年）。

3. 思科，「未來安全遠端工作研究報告」，（思科，2020 年）。