資產管理新知暨法遵系列研討會第一場次活動實錄

主題:「2019 資產管理機構資訊安全實務探討」

為配合金管會打造「金融資安資訊分享與分析中心」提升金融體系資訊安全防護量能，依資產管理人才培育基金與產業發展管理委員會所核定之108年度工作計畫,本基金會於2月20日辦理本年度首場次法遵系列研討會，主題探討「資產管理機構資訊安全實務」，研討議題包括:「國際資訊安全標準與國內相關法令遵循、內稽內控以及風險管理」、「資訊安全實務案例探討」、「2019 資訊安全預測與資安科技導入應用」，分別邀請勤業眾信聯合會計師事務所 萬幼筠董事、永豐金控資安委員會召集人李相臣副總經理、趨勢科技(股)公司洪偉淦總經理擔任主講，最後並安排綜合座談進行意見交流。

本研討會與會者包括：主管機關、周邊單位以及投信投顧從業人員，共計76人參與，研討會主講人分享其國內外資訊安全最新資訊、國內法令遵循、實務案例、風險管理探討與資訊安全預測，並與現場學員交流熱絡。

議程

日期:2019 年 2 月 20 日(三)

地點:臺大醫院國際會議中心 402CD 室（台北市徐州路 2 號 4 樓）

時間	主題	講席
13:30-14:00	報到	
14:00-14:05	主辦單位致詞	證券暨期貨市場發展基金會 李啓賢　董事長
14:05-14:10	貴賓致詞	金融監督管理委員會 張傳章　副主任委員
14:10-15:20	專題演講 1. 國際資訊安全標準與國內相關法令遵循、內稽內控以及風險管理	勤業眾信聯合會計師事務所 萬幼筠　董事
15:20-15:50	專題演講 2. 資訊安全實務案例探討	永豐金控資安委員會召集人 李相臣　副總經理
15:50-16:05	中場休息	
16:05-17:00	專題演講 3. 2019資訊安全預測與資安科技導入應用	趨勢科技股份有限公司 洪偉淦　總經理
17:00-17:20	綜合座談- 2019 資產管理機構網路資訊安全實務應用探討	主持人: 金管會資訊服務處　蔡福隆處長 與談人: 勤業眾信會計事務所　萬幼筠董事 永豐金資安委員會召集人　李相臣副總 趨勢科技股份有限公司　洪偉淦總經理

主辦單位致詞

證券暨期貨市場發展基金會　李啓賢董事長

李董事長開場致詞表示：目前資訊安全議題在我國已上升到國安層級，在各行各業中過去談到資安多半認為較偏向資訊技術方面的領域，但如今已擴大到包括:風險管理、內稽內控、法遵等各部門都息息相關。

在 2018 年行政院正式通過「資通安全管理法」後，金管會也隨之研擬推動通過多項相關規範，並要求各級金融機構都必須設立資訊安全的專責單位及負責主管，相信在逐步落實建立資訊防護網絡措施之下，未來將可大幅減少相關資安風險事件發生的機率及所導致的損失。

貴賓致詞

金融監督管理委員會　張傳章副主任委員

張副主任委員提出:金融科技 Fintech 的浪潮目前正在全球不斷地翻新金融業的樣貌,是典型的破壞型創新。在金管會的立場,希望這樣的創新建立在資訊安全無虞、且能充分保護消費者權益的「負責任的創新」。

有鑑於此,在加強資訊安全的考量下,金管會提出了五項措施要求金融機關更加重視資訊安全的維護,包括:

1. 將資安實施成果作為新業務申辦的准駁依據;
2. 資安成效作為資本計提的參考;
3. 金融機構必須設立資安專責單位及主管,且做合理的資源與人員配置;
4. 董事會內強化資安治理架構;
5. 金管會也將隨時因應市場變化進行金融監理資安妥適性的機動討論。

張副主任委員並期許所有來自金融界資安業務的代表們,能透過本日研討會與業界最優秀的資安專家深入交流,強化資安方面的知識,並能更進一步提升金融資安的水平。

專題演講 1.「國際資訊安全標準與國內相關法令遵循、內稽內控以及風險管理」

勤業眾信聯合會計師事務所　　萬幼筠董事

國際資訊安全法規趨勢

萬幼筠董事彙整說明表示:在國際資安法規上，全球各主要國家都已經對資安風險升高的趨勢有所認知，所以包括美國「聯邦資訊安全現代化法案」、「歐盟網路安全準則一般資料保護原則(GDPR, General Data Protection Regulation)」、中國「網路安全法」、新加坡「網路安全法」等；而我國也在 2018 年正式通過「資通安全管理法」，足見各國都已認知到資安問題應正視落實到法律層面來加以管控。其中在個人資料隱私保護方面，自從歐盟實施 GDPR 後，因為影響層面已擴及到全球，各國為進行國際接軌以確保本國企業在國內外進行跨境活動時遵守的法令標準一致，也紛紛推出各國不同的版本，如美國、中國、日本等，所以企業間已不能再將保護個人資料的任務因業務地區不同而有明顯的區別。

國內資訊安全相關法規

萬董事並對受影響較大的法令與函釋方面表示:目前法令急需各金融機構注意的包括:1.「金融控股公司及銀行業內部控制及稽核制度實施辦法」第三十八條之一第一項；2. 107 年 5 月 30 日修正「證券暨期貨市場各服務事業建立內部控制制度處理準則」第 28 條及臺灣證券交易所 107 年 7 月 24 日修正「證券商法令遵循之評估內容與程序標準規範」

萬董事進一步說明我國「資通安全管理法」的內容及架構:首先本法令主要規範的對象是以公務機關,包括中央與地方機關以及公法人;以及特定非公務機關，包括關鍵基礎設施提供者(能源、水資源、通訊傳播、交通、金融、高科技園區)、公營事業，以及政府捐助之財團法人等。整體架構則以資通安全推動組織、公務機關、特定非公務機關資安管理、資安整體環境與產業發展，以及最容易忽略的

資通服務之委外管理。在執行架構上，公務機關的執行重點在於「提出並落實有效的資安維護計畫」；而特定非公務機關的責任則在於「建立有效率的通報應變機制以及後續如何進行調查、處理及改善報告」。

資訊安全科技運用與風險管理

法遵人員在資安議題上，應建立法令遵循作業標準、導入特定法令遵循風險評估與控制之外,對內的訓練與溝通以及熟悉各類支援性技術:如法規監控工具、法規資料庫、持續性監控平台、舉報系統等都是技術性含量極高的挑戰。過去法遵人員在評估法遵風險及法規變動之影響性時，需花費龐大的人力與時間成本，來比對內外規的條文內容，但如今在大數據科技及人工智慧的輔助下，將內外規資料進行數據處理，非結構化數據轉化為結構化數據，利用人工智慧文本分析技術，使法遵人員在進行法遵風險及法規變動影響性評估時，大幅降低所需花費的人力與時間成本。因此，這也將是有效發展資安法遵系統的極佳契機。

專題演講 2. 資訊安全實務案例探討

永豐金資安委員會召集人　李相臣副總經理

個資外洩事件

李相臣副總經理首先談到「衛生局公衛系統市民個資於暗網兜售事件」，其委外資安業者在進行演練期間，發現地下網站有人販售衛生局個資，其中可能包括藥物及化粧品線上查詢暨申辦、行政資訊、健康管理個案管理系統、精神病患管理系統等資訊。後續市政府表示，雖已委外資安業者完成掃毒，但對於本案的成因，究竟這是所謂的 APT（進階持續性威脅），還是針對式攻擊，都還未能真正確認，仍需更深入的調查才能有真正定案。

駭客盜領事件

李副總經理舉出某銀行在 2017 年時被駭客透過 SWIFT 系統盜領，瞬間盜轉 18 億元的事件，後來被證實此案是來自北韓專門在全球各進行駭客攻擊的 Lazarus 組織，之前也曾參與 2014 索尼影業內部電郵外流的事件、2017 想哭勒索軟體遍傳全球以及後來 2016 年孟加拉央行在美國紐約聯準銀行帳號 8000 萬美元盜領等事件。從本事件中，暴露出 SWIFT 在國際通匯的領域上存在有極大的資安問題，且在 2013 至 2016 年間全球已發生至少 6 起類似的 SWIFT 盜領事件，所以李副總提醒國內金融機構務必需對此一風險高度重視。

ATM 盜領事件

有關一銀 ATM 盜領事件，李副總說明本案基本上分成許多不同的環節，且由個別不同的人員負責執行，從系統面的入侵分行 PC、入侵分行系統主機、入侵派送主機、入侵 ATM，到後端的車手至不同 ATM 領款，後續的洗錢都由高度專業的外籍人士策畫執行，真正做到跨國專業分工。就在一銀案後，同樣的手法也陸續發生在俄羅斯以及泰國的 ATM，也可見 ATM 系統亦成為全球駭客有高度興趣的目標。

券商遭受 DDos(分散式阻斷服務攻擊)駭客勒索事件

駭客在 2017 年針對台灣券商交易系統進行 DDos(分散式阻斷服務攻擊)，當時有近 10 家券商受到影響。當時駭客是藉由越南做為跳板發動攻擊，雖然當時並沒取得贖金，但極有可能導致駭客日後將攻擊層次升級到「加密系統」，也就是將受攻擊者的系統「上鎖」，無法正常使用。而類似的方式在前一年 2016 年就曾經有一名 23 歲學歷不高的年輕駭客，透過「自學」的方式向國外直接購買服務工具，利用 DDos 的方式向某金控勒索比特幣，並成功得手 100 個比特幣。

資案攻擊事件的預防

綜合以上各個案例，李副總表示要有效執行資安管理，重點不在於資料量的多寡，而應在於如何分析資料。資安人員應有能力獨立進行識別、防護、偵測、應變到復原等各階段的作業，而不應透過委外完成，造成另一個不可掌握的風險產生。未來更有必要運用大數據分析，來從 Email、USB、Web 找出讀取病毒者、從資安健檢中找出中毒者，最後則是從攻擊分析中找出釋放病毒者，進行阻隔或追查，並在科技管理與效率創新真正找到最合適的平衡點。

專題演講 3. 「2019 資訊安全預測與資安科技導入應用」

趨勢科技　洪偉淦總經理

2018 年重要資安議題回顧

洪偉淦總經理首先回顧 2018 年全球最主要的資安議題:

1. 挖礦病毒:

如透過 MS17-010(網路芳鄰)弱點散布 Fileless 挖礦病毒，及對外提供服務的伺服器被植入挖礦病毒等方式。

2. 勒索病毒:

雖然隨著企業及使用者已有隨時建立資料備份的觀念因而減少這類案例，但是另一種目標式勒索的案例卻仍有增無減。尤其是舊的蠕蟲病毒仍持續潛伏在許多製造業的伺服器主機內，利用這類蠕蟲所進行的攻擊主要是對製造業造成很嚴重的生產中斷的影響，而且發現的案例也越來越多。

2019 資安議題與趨勢

洪總經理也就 2019 資訊安全議題趨勢與現場參加人分享:

1. 網路釣魚攻擊模式:

因為目前沒有一種作業系統能在所有的 IOT 設備中佔有超過 50%以上的市佔率，過往駭客喜歡使用漏洞式攻擊，針對 Windows 系統所進行的攻擊已經顯得效益沒有那麼高;目前許多駭客就改以網路釣魚的模式來進行攻擊，尤其是透過社交工程，包括電子郵件、聊天軟體、社群網路等方式，已變得相當常見。

2. 網紅文化盛行個人帳戶成為資安漏洞:

單一社交網站網紅帳號通常聚集大量流量或交易，非常容易吸引駭客的注意；再加上網紅多半是個人經營，在資安的維護能力也遠低於企業，所以更是駭客眼中的肥羊，其中有的模式就是搭上目前的挖礦

熱潮，利用網紅帳戶植入病毒在進行虛擬貨幣挖礦，竊取大量的運算資源獲取利潤。

3. 新興駭客攻擊模式:

預期在今年會有更多的憑證填充攻擊或是 SIM 劫持手法來取得個資，再對不同的金融、社群網站發動攻擊來進一步獲取資源或利潤，使得受害範圍變得更廣且更難在第一時間查到資料外洩的源頭。

4. 在家工作個人電腦系統造成資安風險上升:

因應新的工作型態改變，越來越多企業容許員工可在家工作，也使得企業面臨更多的 BYOD(自帶上班設備風險)，變臉詐騙(Business Email Compromise)的對象也會因此擴大。

前述的網路釣魚、社交工程、憑證填充攻擊以及 SIM 卡劫持攻擊也正好是金融業最常會碰到的駭客攻擊模式，最主要的目的則是入侵商業流程。最著名的幾個案例如:Target 數據外洩事件、徵信機構 Equifax、孟加拉央行被 SWIFT 盜領、日本 ATM 盜領等，都是金融業會面臨到的各種駭客入侵樣態。

洪總經理同時也舉例，這裡面最難察覺的一種攻擊是 APT 攻擊軟體，這種惡意程式因為是客製化的，不僅一般防毒軟體無法辨識，連防火牆或入侵偵測都無法察覺跟阻隔，而且甚至還會潛伏在企業的伺服器內非常長的時間都不一定會真正展開攻擊；短則一年，長的甚至有 10 年以上的紀錄。

資訊安全防護與資安風險降低

洪總經理認為:企業應該要有的認知就是資安不可能 100%安全，而是要如何將風險降到最低，以及在事件發生時能有最佳的應變處理措施；沒有資安事件，並不代表你並沒有被入侵，更有可能的是你已經被入侵但還沒有發現。

企業高階管理階層對於資安應該要清楚認知:這並不只是技術問題,而應該是風險控管議題，資安必須結合人員、流程、及技術才能有效解決，這更是企業全體的工作，需要的是各部門的共同配合。

洪總經理並提出整個資安防護架構的重點工作系統包括:1.威脅情資的收集與分析、2.委外單位的控管，都必須在有完整的威脅辨識、防護、偵測、應變以

及修復的流程下快速且有效的運作，才能真正將資安風險降至最低，達到最佳的防護效果。

綜合座談：「2019 資產管理機構網路資訊安全實務應用探討」

主持人：　金融監督管理委員會資訊服務處　　蔡福隆　處長

與談人：

勤業眾信聯合會計師事務所　　萬幼筠　董事

永豐金控資訊安全委員會召集人　　李相臣　副總經理

趨勢科技股份有限公司　　洪偉淦　總經理

本次座談會交流議題如下：

問題一、應如何讓金融機構從上而下做到真正形塑重視資安的企業文化?

萬董事回應表示:金融機構高階管理者在做系統的資安跟業務間的權衡評估時，常為爭取市場佔有率，而沒有做到足夠的評估就將系統上線，導致資訊系統只有功能規格，卻缺乏完整的安全規範，因此高階主管應該重視此議題，且應該要在各部門間做協調整合，並且有良好的系統規劃與完整的評估，且週期性的作檢討評估與資訊安全宣傳推廣，讓資訊安全變成所有內部員工的基本知識。

問題二、資安議題貌似重要，為何卻總是在真正出了大事件後才會受到關注，如何能讓高階管理者持續關注資安的維護及執行上?

李副總經理指出:人們是健忘的，高層管理者常在事情發生後一段時間，開始質疑為什麼要花這麼多資源放在看不見績效的資安上，李副總經理分享其做法，基本上會每 2~3 個月針對資安的不同主題，包括人為因素、系統或作業層面等議題，對高階管理層進行上簽，讓公司高階管理層能持續就資安議題進行討論，維持應有的關注度。

問題三、當資安事件發生時，金融機構應在第一時間做甚麼樣的處置並如何與外部資安公司展開合作?

洪總經理表示:雖然資安在金融機構通常會有專責資安部門主管負責,但當事件發生時，也就代表資安主管可能也是第一個會被追究責任的對象，導致真正要整合內部資源開始對敵作戰時，反而會出現沒有指揮官的窘境，這也會導致光是要找到真正能負責指揮全局並協調各部門就要花很多時間，錯失黃金處理時機。所以他建議，各機構應訂定一套標準流程，規定一般時間的組織架構以及真正發生事件的「戰爭時期」的組織架構，這樣可以防止再群龍無首時，導致危機擴大的情形發生。

講義電子檔下載(PDF):

專題 1.國際資訊安全標準與國內相關法令遵循、內稽內控以及風險管理