Part 2：綜合座談

後疫情時代 以網路安全及資訊韌性迎戰資安威脅

2020 BSI InfoSec Standards 國際資安標準管理年會

責任編輯 徐瑋琳 | 撰文整理 鄭詠中 | 修正校訂 黃純郁

BSI 國際風險管理年會於 2020 年 11 月 26 日舉行，本屆主題聚焦於「後疫情時代 以網路安全及資訊韌性迎戰資安威脅」。去年推出的「資安管理劇場大探討」綜合座談大獲好評，大會今年再度邀請揚名海內外的資安高手、國家資安政策掌舵者及國際標準制定者進行座談，精選來賓投稿的資安劇情，由不同專業領域的專家現場解讀資安病徵，指出改善方向，優化資安管理績效。座談重點內容整理如下：

綜合座談【你的情境，我的借鏡】

資安管理劇場大探討

主持人：BSI 英國標準協會東北亞區 蒲樹盛（Peter Pu）總經理

與談人：金融監督管理委員會資訊服務處 蔡福隆處長、奧義智慧科技 邱銘彰創辦人（Jeremy）、永豐金控專業董事暨中華民國電腦稽核協會理事長 葉奇鑫律師、BSI 英國標準協會 孫文良客戶經理（Sunny）

「你的情境，我的借鏡」是資安管理劇場大探討的中心概念與用意，活動前收集各方資安疑問投稿，就共時性提問，請各界名家提供解決方案與視野，並就策略、管理、技術、法遵四個面向，探討資安風險。

「資安管理劇場大探討」，左起：BSI 客戶經理 Sunny、奧義智慧科技創辦人 Jeremy、金管會資訊服務處處長蔡福隆、永豐金控專業董事暨電腦稽核協會理事長葉奇鑫，以及 BSI 東北亞區總經理 Peter。

Q1 金融單位依法設立了資安長，但資安長底下也沒有其他人了，這如何對組織有所幫助？

蔡處長：按「金融資安行動方案」，一定規模以上（資本額超過一兆）的金融單位需專設部門負責資安，部門負責人需為處長或協理以上之高階主管，一般規模金融單位，則由副總兼任資安長，使高階主管負責資源調配以及資安工作支援協調，從組織面向推動資安。

葉律師：本身為兆豐金控專業董事的葉律師，並負責總統府資安稽核，表示稽核第一要項在組織，就資通安全法，資安專責部門負責人產生後，預算編列與計畫也會隨之而生，制度都是循序漸進，且金融界的資安要求在國內各產業已是最高，可為各界示範。

Q2 資訊與資安的分工—資安防禦設備從採購到後續的管理責任，究竟屬資安或者資訊部門的工作？

Jeremy：大部分公司是先有 IT 才有資安，因此大部分的資產設備是由 IT 部門在掌管，但稽核與資安部分的營運又是由資安部負責，資訊與資安人員會產生衝突是事實；許多傳統產業的資安能力沒有隨企業演化的進程提升，且學校培養的資安人才重在技術而非實務上的治理，都是當前資安與資訊權責難以界定清楚的原因。

Sunny：建議由「分工合作」切入，類資安但偏可用性功能性的網通設備，由資訊專業部門來維護，獨立的資安設備（像防火牆），當屬資安；若真的要應用到網通設備上的存取控制功能，可把過程交由資安單位作安全控制審查，再由資訊單位實施設定，以專業責任分工。

Q3 近兩三年金融界在資安預算人力不足（按 iThome 問卷結果），「金融資安行動方案」有哪些和資安治理與預算有關？

蔡處長：金管會對金融機構提出的「金融資安行動方案」，其實是有相當多的要求與工作事項，金融業在今明兩年的相關預算或許是會有相當程度的增加；透過金融機構本身的資安治理、強化金融韌性，讓相關資安工作做得更落實，是這個計劃的精神，未來資源及預算的投入只會增加不會減少。

Sunny：金融業就一般產業來說資安預算是最高的，監管機關要求和設計上，可預見投資應會增加，尤其是「人」的投資，如何獲得條件具備的人才，現狀是人才都

聚集在資源多品牌高的企業，有些單位資源薄弱拿不到人才，或許可先從組織內人員培養，並詢問專家學者，釐清自己的需求開始。

Q4 目前很多營業秘密，資安人員十分容易接觸到—在營業機密與員工競業禁止條款間，有何規定？（來自製造業的提問）

葉律師：是否可限制知曉核心技術員工前往競爭企業任職？答案是可以（詳情請參照勞基法）；資安是對外的防護，防火牆內的內鬼更難防，若員工不願意簽訂競業禁止合約，資安做得好，員工有動過任何手腳皆有完整的紀錄，只要跳槽即可提出告訴；競業禁止合約第三項「秘密性」舉證最難，若資安防護設定可以顯示出組織有盡最大義務注意與保護（像是不只要經過刷卡，資料取得要經過一定的程序），律師舉證就容易得多。

Jeremy：以上一份在以色列資安公司經驗分享：為返台進行新創，離職前原服務公司讓 Jeremy 簽訂了厚厚一份合約，等於是「井水不犯河水條款」—明定 Jeremy 返台成立新創公司，一定時間內技術與業務不得與原公司重疊。Jeremy 公司於 2020 年也剛通過 ISO 27001 的驗證，公司僱用人員進公司就要持續教育資安意識，並做無犯罪紀錄申請，有關客戶的資訊必須在特定的會議室內進行談論，這對客戶都是一種保障。

Q5 請教蔡處長與葉律師，分別從法遵和金控董事角度看 BCM（營運持續管理系統），「金融資安行動方案」是否鼓勵企業導入？

蔡處長：一般公司通過 ISO 27001，應該是都具備了 BCP（營運持續管理計畫），但有些 BCP 範圍很狹隘，可能是以 IT 為主的備援，並未考量到各種情境的天災人禍與風險，這樣的 BCP 是不完備的。未來金融機構的 BCM 應該是要從組織的架構來去看如何達成營運持續，像是 ISO 22301 營運持續管理系統從組織架構、業務、財務、IT 等部門，一同檢視災害備援措施，這是金管會看到的議題，演練時連同金融周邊單位也同時進行。

葉律師：從組織董事的角度當然是贊成，董事會的風控報告案會針對特殊的事件做出風險預測，像永豐金控在今年初就將 Covid-19 的風險分為嚴重、極嚴重、超級嚴重這三個情境，去預估事件發生時組織的資本適足率是否足夠，各事業群也會再另外訂定相關的因應辦法，但要做到穩定的持續營運，不能只從各單一部門自身專業去努力，而是多方整合，就各種各樣的面向，所有人員配套上去做規劃。

Q6 一般駭客對供應鏈攻擊，要如何防禦？

Jeremy：企業使用的元件軟體從何而來，需用流程檢驗；RD（研發單位）的資安意識需教育提升。

Sunny：資通安全法規範組織單位須對供應商盡監督之責，大型供應商本身在業務考量下就自我管理嚴謹，而導入 ISO 27001 的單位至少就其特定範圍有一定程度的管理流程；若只能委託資安資源較少的供應商時，也可提出指標性案例做法作為參考，幫助供應商就是幫助自己。

Q7 資安法很重要的一環在個資隱私保護，可否請葉律師就可公布範圍內與大家分享目前法令相關情況？

葉律師：身為國發會個資修法委員，葉律師說明原考量歐盟對法規適足性要求的背景下，國內個資法朝歐盟個資法（GDPR）方向修訂，且需達成兩個目標：1.法律強度要和 GDPR 差不多；2.要有獨立專責主管機關。並舉之前 CHANEL 德國分公司，人資利用大數據分析同仁上班時間行為，以提升工作效能，但搜集資料前未先告知同仁，按 GDPR 被裁罰三千多萬歐元，是以年營業額 4%計算。台灣目前個資法主管機管有三個，又遇上 Covid-19，原訂修法方向是否有變動還在觀察中，影響民生企業的法案變數總是很多。

系列文章：〈後疫情時代 以網路安全及資訊韌性迎戰資安威脅─Part 1：會後報導〉