Part 2：講座摘要

當風險串成鏈──用「Link & Break」思維提升防駭力、應變力與管理力

2018 BSI InfoSec Standards 國際資安標準管理年會

責任編輯 徐瑋琳 | 內容修訂 黃純郁 | 採訪撰文 鄭詠中

2018 年 BSI InfoSec Standards 國際資安標準管理年會，在 12 月 6 日於張榮發基金會國際會議中心舉辦。會中舉行 BSI Excellence Award 卓越組織表揚典禮，肯定企業在資安方面實實在在的努力；並精心安排「資訊安全」與「網路安全」相關議題的講座，根據全球管理趨勢、企業需求與時事趨勢，邀請產官學研界的菁英專家進行分享，協助國內企業組織互相交流、接軌國際。

一、【生存家的智慧】全球科技風險與組織韌性解析

首先登場的是 BSI 台灣蒲樹盛（Peter Pu）總經理。兼具淵遠人文歷史與尖端科技趨勢涵養，是蒲總最迷人之處。蒲總一上台就問全場：現今世上經營最悠久的企業有多少年了？答案是位於日本京都的金剛組廟宇修繕事業，該企業已經營了 1400 年之久。企業如何歷久不衰，端看它如何因應時代更迭、環境變遷，如何面對無處不在的風險。

資安講座首先登場的是 BSI 台灣蒲樹盛總經理，以永續經營切入談科技風險與組織韌性。

2018 年全球風險排名第一的是環境風險：按該年 10 月聯合國《地球暖化 1.5℃報告》，全球暖化攸關生死存亡—2030 年，達暖化大限，地球平均溫度增加 1.5℃，我們只剩 12 年。隨著平均溫度增升，傳染病也面臨難以控制的變數。人們自工業革命起發展的過程，破壞了地球環境，打亂了社會經濟，面對與日俱增的變化與突發性的崩潰，組織需具有預期未來、做好準備、因應及適應的能力，讓組織得以生存及成功。說穿了就和達爾文演化史的結論一樣：「適者生存」（蒲總補充帶到台灣的情況：因為太想要一下就變強，以至於韌性不足。）

企業的生存力取決於「組織韌性」（Organizational resilience），包含三個要素：產品、流程、人員；三個領域：營運韌性（Operational resilience）、供應鏈韌性（Supply chain resilience）、資訊韌性（Information resilience）；以及 16 項被視為組織韌性策略的核心指標，企業可以參照 BS 65000 標準自行評估，也可以委由外部單位進行以更詳實的瞭解組織競爭力，找出可以改善的方向，提高相對競爭力。

2018 年資安風險也在全球風險排名中上升，台灣從法遵面透過於 2018 年 6 月 6 號公告的資通安全管理法予以因應。企業已無法背離資訊，其中的資安問題絕不是企業組織唯一面臨的風險，但若是連資安這項成長最快的風險都無法掌握，更遑論許多其他風險都遠超過我們的能力。

最後，蒲總以 2011 福島核災報告與大家分享─2016 年，經過細膩的調查與追蹤，福島核災五年後，完整的事件報告終於出爐。大家都以為是因為天災（海嘯），造成了此次鉅變，但報告中指出，其實是人禍：福島核電廠決定性的管理階層本身專業度與敏感度不足。再加上關關層層連帶的人為干預，導致緊急應變措施無法貫徹執行，導致震驚世人的「福島災變」─蒲總想用這個時代性的災變與大家共勉：福島兩座核能電廠有同樣的 SOP，但因為核災應變程序落實的程度不同而導致不一樣的結果。這就是組織韌性，在關鍵時刻做出正確的應對與堅持，生存下來，把災害降到最低。(下載講師簡報)

二、【國家資安戰略】資安威脅趨勢與防護策略

第二場講座，請到了行政院國家資通安全會報技術服務中心吳啟文主任，談國家資安戰略。吳主任也從 2018 全球十大風險調查談起，科技類的「網路攻擊」與「資料詐欺或盜竊」的排名都更勝 2017 年。將全球資安威脅主因攤開來看：從 APT 進階持續威脅攻擊竊取機密資料、DDos 分散式阻斷服務攻擊癱瘓網路運作、IoT 物聯網資安設備弱點威脅升高、關鍵資訊基礎設施資安風險倍增、網路與經濟犯罪影響電子商務與金融運作、偽裝 APP 向行動錢包發動攻擊，與資安（訊）供應商持續遭駭客破壞供應鏈安全，每一個區塊都有該年度對應的本土或國際經典案例。吳主任說明，以往機關單位以為自己是封閉的系統，事實上只要有連結網路，都能攻破，從印表

技服中心吳啟文主任，從威脅實況談國家資安戰略與因應法規。

機、網路攝影機、門禁系統，到能源系統、電力系統甚至是水資源系統都無一能免。關於政府的資安威脅，本來就持續存在，較常見的攻擊之一是針對負責國防、外交、經濟等機關機要秘書，利用社交工程植入惡意程式，趨勢也顯示開始鎖定具有管理權限的系統管理人員。

分析 2018 年 222 件政府機關資安通報案例，非法入侵事件佔 45.5%。原因主要為疏於管理和網路暴露：近年來由於政府提供的服務 App 越來越多，活動結束後又沒有安全下架、測試環境未限制網際網路控管存取；或者部分受害設備轉作 IoT 設備與工業控制系統；或者透過中繼站、共用性系統與雲端服務攻擊，建立灘頭堡、竊取內網通行證、進行共用性系統通行證、進行跨機關全面滲透，達成機密竊取。

從正面的角度觀察，過去公務機關覺得資安風險是資訊單位的議題，但現在已意識到資安風險就是機關風險，資安就是國安，也將資安提升到資安「治理」的層級。機關首長需要重視資安，包含資安目標與機關的目標能否結合，相對的資源人力能否配合。面對日趨白熱化的資安攻擊，資通安全管理法（以下簡稱資安法）因運而生，提案過程也相對順利，期在民國 106 到 109 年，以打造可信賴的數位國家為目標。立法目的與規範對象：個資法分為公務機關與非公務機關；資安法規範對象分為公務機關與特定非公務機關。其中，具有多重身份的機關比較會面對複雜的情況。透過網路攻防演練與資安全年稽核精進防護系統，並將國際資安訊息以國家 N-ISNC 層級通報分享給機關及八大關鍵基礎設施提供者（政府機關/高科技園區/通訊傳播/交通/水資源/能源/醫療/金融），並建立地方政府區域聯防以及國家資安聯防系統。

吳主任最後也談資安法整備重點與因應建議，目標是透過這套專法，以「事前」、「事中」和「事後」不同的因應措施營造國內資通安全環境，保障國家資通安全。吳主任細細講述資安法整體架構內容，六個子法從先期規劃、持續運作、通報應變到協助改善類似於 PDCA 的精神，都是當下能把握且實行的範圍。如同非洲豬瘟對台灣畜牧產業及其供應鏈造成的威脅，從產業到全民都有警覺意識，巨大的風險反而可成為團結一致的契機。

三、【經驗分享】數位金融安全的思維與作為

第三場講座，請到了第一銀行劉培文副總經理。相當有緣分的是，劉副總曾經在技服中心任職十二年之久，兩年前被禮聘至第一銀行負責資訊安全，並進一步落實銀行數位轉型計畫。基於跨界經歷，以 outsider 的角度看金融界的資訊安全，劉副總做了以下比喻：資安重大事件，如同颱風與地震，會獲得高層最即

時性的關注；數位轉型，如同地球暖化，對高層來說不忙的時候可行，忙起來的時候不行。妙喻一出，滿場歡笑。

第一銀行劉培文副總經理提醒大家:「不要迷信最新的 solution，聯防才是重點。」

從這兩年全球重大金融資安事件說起，劉副總破題指出：資安一定要打團體戰，國家的資安政策一定要見樹又見林，希望政府能鑑別與建立起每一個產業的資安風險領域。隨即以自家第一銀行為案例，檢視之前重大資安事件，劉副總到職上任後做了哪些措施──過去第一銀行跟許多同業一樣，資安人員就隸屬於資訊部底下的安控部門，工作重點可能放在合規，但沒有人員與能量去做資安的監控與應變。劉副總到任後將資安層級拉高，成立了數位安全處，並規劃出資安管理部負責資安政策、程序、管理與稽核，另外還成立了安全技術部，也就是電腦安全事件應變團隊（CSIRT），就是要有能力從外到內的資安情報做搜集、分析、處理，並在意外發生時做出應變。劉副總同時也提醒大家：不要迷信最新的 solution 或設備，每一種 solution 都有它最強的地方，也會有其弱點，如何串連各種設備，如何聯防才是重點。

繼續金融資安領域詳析。劉副總說明，銀行最強的是安全控管，但安控不等於監控。目前銀行的資安監控與安全控管是分開的，還有很多不同的安全風險需要關注，希望能有一套框架，能夠將銀行所面臨的各式風險做整體性的監控。然而光有資安設備和管理措施還不夠，還需要以資訊安全三道防線─資訊作業安全控管、資訊安全規劃及監控、資訊安全稽核管理來推動資安，更需要董事會的政策支持，讓資安部門擁有權限對各業管單位做定期檢查並向董事會報告。其實美國的 NYDFS 500、香港的 C-RAF 及歐盟 GDPR 規範內也都有這些機制，這麼做並非只是為合規而合規，而是想要真正的做好資安。劉副總並提供了資安成熟度評估圖表供大家參考：從評估計畫與預算的規劃、到控管框架、建置完整度、企業文化與員工心態、事件處理能力、威脅管理與修補能力等通通涵蓋其中，要讓高層能看到投入資源後的資安優化進程。

接著談數位金融轉型。網際網路與雲端技術的發展讓新型態的金融科技業者獲得成功的機會。相較於傳統銀行，新創金融單位在資訊人事成本低非常多，在此利基點上，新創的 Business Model 不需提供所有的金融服務，反而可針對銀行的痛點去做單點服務，這種破壞式的創新一但做起來了，挾著這樣的利基跨入傳統銀行業務，傳統銀行就得面對直接的衝擊。劉副總進入最後結論：以自身 CIO 的角度來看，People / Process / Technology 永遠是我們要掌握的，除了聚焦

資訊安全、數位轉型、如何進行資訊現代化，更要思考的是如何將業務單位的金融流程知識以及資訊單位的數位競爭力，轉移給業務單位的企劃人員，讓他們也能夠具備數位的 DNA。明年第一銀行就要成立滿 120 年（全場掌聲雷動），成長過程中當然面臨過許多事件，重要的是去思考未來面臨的挑戰是什麼，要如何應戰，無論是資安議題或是數位轉型，韌性 resilience 將是企業非常需要的能量。（下載講師簡報）

四、【扭轉危機的實力】用廣度、深度及速度提升資安治理成熟度

BSI 台灣謝君豪營運長帶著招牌笑容，替大家整理出如何透過國際標準與指引，讓組織混亂的資安現況，理出頭緒得到最適切的解決。

最後一場講座，由 BSI 台灣營運長謝君豪（Joe Hsieh）壓軸登場，Joe 帶著招牌笑容在台上與眾人問好，接著 show 出近年來資安重大風險案例，直接要談的是在這個風險與機會並存的數位年代，放眼歐洲北美與東協，網路安全皆為影響產業發展的首要因素，持續進化並交互作用的數位應用同時替資安人才的需求帶來變革，不僅要專才，還需要許多知識來維持資安人才的專業競爭力，也才能有效因應多面向的資安風險。資訊安全的有效管理至今已是展現企業良善治理的關鍵，從各產業界所編製的 CSR 企業永續報告書中可看到，客戶權益與資訊安全、隱私保護與交易安全，是為利害關係人關注的焦點，一但資安做不好，商譽必然受損。

Joe 分享了一些稽核案例，與會來賓聽完會心一笑但也都心知肚明，這種發展算有規模但資安能量不足的企業在國內並不少見。要提升企業在資安治理的韌性與成熟度（策略、管理、技術及認知各方面），要先建立制度與資安文化，避免便宜行事與提升落實度。在降低社交工程攻擊風險方面，Joe 又提出幾個常見 E-mail 案例：包含一例一休、減重等看似有用而無害的信件主旨，問現場誰會開啟？即使嘴上不說但心裡其實明白，大家在日常資安警覺度和堅持度都不夠高，十分容易被擊破。透過國際標準及指引提升企業在資安治理綜效，是在現實混亂中理出頭緒，爬梳紋理找出方法的救命浮木：

- BS 31111:2018 網路風險與韌性──替企業導入必要的成熟度模型並評鑑。

- NIST CSF 美國網路安全框架——透過五大功能，辨識/保護/偵測/回應/復原，替企業理出應強化的範圍與優先順序，步步實施行動計畫。
- ISO/IEC 27001 + NIST CSF 美國網路安全框架——評估企業網路安全控管成熟度。(緊急應變能力是台灣產業的相對弱點，此項標準能協助企業展現風險控管成熟度)
- ISO/IEC 27001 + 隱私相關指引與標準 (ISO 29151、BS 10012、ISO 29134)——強化組織對隱私衝擊分析的能力。從數位化服務出現以來，隱私保護與資訊安全劃上等號，確切的分析與相對應的處理是企業必備戰力。
- ISO/IEC 20000-1:2018——品質與安全的界限越來越模糊，資訊部門如何展現績效？Joe 替大家畫重點：品質顧好了安全也會強化，這就是 service assurance。
- ISO/IEC 19086-1~4 雲端服務水準協議 (SLA) 系列——Joe 一言以敝之：這個系列就是幫助企業，展現您的雲真的做得很好。

Joe 還從自身使用智能手錶記錄每日步行數上傳雲端，獲得健康保險續約減額；新居智能家庭系統設立，在考量到資訊安全的底線之下所做的取捨為實例，都在告訴大家：資訊安全並不是一個專門的產業用語，是數位時代無所不在的實相與覺知。再複雜多樣的標準版本，Joe 都能談笑間輕鬆對應到產業現實的挑戰與困境，做最精確的連結指引，聽眾都覺得收穫豐富。

※ 延伸閱讀→〈當風險串成鏈：用「Link & Break」思維提升防駭力、應變力與管理力─Part 1：會後報導〉

BSI 資訊安全與網路安全系列課程

資訊安全	個資管理	雲端安全	品質管理	營運持續	產業資安
ISO 27001 資訊安全管理系統 基礎課程 建置課程 風險評鑑課程 內部稽核員課程 主導稽核員課程	BS 10012 個人資訊管理系統 基礎課程 建置課程 內部稽核員課程 主導稽核員課程 主導稽核員/稽核員轉版課程	雲端服務資訊安全管理系統 Cloud 主導稽核員課程	ISO 20000 IT 服務管理系統 基礎課程 建置課程 內部稽核員課程 主導稽核員課程	ISO 22301 營運持續管理系統 基礎課程 主導稽核員課程	PCI DSS 支付卡產業資料安全標準 以 PCI DSS 強化電子支付服務的資訊安全管理及法規遵循課程 內部稽核員課程 主導稽核員課程
GDPR 歐盟一般資料保護規範 基礎課程	ISO 29100 隱私框架基礎課程 主導稽核員課程	ISO 27017 & ISO 27018 建置課程	NIST 網路安全框架 建置課程	BSI 營運衝擊分析課程	ISO 27799 健康醫療資安基礎課程