Part 1：會後報導

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

由 BSI 英國標準協會主辦的「2020 BSI 國際資安標準管理年會暨表揚典禮」，2020 年 11 月 26 日於張榮發基金會國際會議中心舉行。BSI 東北亞區總經理蒲樹盛（Peter Pu）上台致詞，話及當年在 ISO 27001 前身 BS 7799 推出時，對資安要求僅限於機密性、完整性與可用性，隨資安環境複雜度逐年升高，「資安管理」必須提升至「資安治理」，點明主題「後疫情時代下的資安新常態」：Covid-19 促使數位化轉型，資安風險劇增；釣魚信件頻傳、駭客攻防升級，法律遵循亦納入資安挑戰──年會從管理策略及流程面出發，搭配務實名家觀點，探討資安風險與治理，分享如何培養出「網路安全與資訊韌性」，迎戰資安威脅。

金融監督管理委員會資訊服務處蔡福隆處長，以「亞洲公司治理評鑑」台灣榮獲排名第四的佳績，帶出金管會「金融資安行動方案」[1]，建議金融單位導入 ISO 27001 資訊安全與 ISO 22301 營運持續管理系統，藉國際標準達成治理績效之期許。本屆典禮受獎單位包含網路科技、電子通訊、金融、醫療、汽車租賃、公部門與法扶等跨領域組織，恭喜所有得獎企業，藉由導入資安國際標準，訂定資安策略與管理施行，提升技術完成法遵，奠定資安治理基礎。

資安保護深耕獎（上）和營運持續遠見獎（下）受獎代表與 BSI 蒲樹盛總經理合影留念。

[1] 2020 年 8 月 31 日，金管會宣布「公司治理 3.0─永續發展藍圖」正式啟動，一定規模以上的金融單位董事會需設一名有資安背景的獨立董事，並建議導入 ISO 22301 營運持續管理系統。有鑒於駭客攻擊不只針對於金融單位，早已擴及科技大廠與其他產業，相關要求也可適用於所有珍視公司資產的企業組織。

專題演講 1【資安新常態】

營運持續與韌性全球趨勢

主講人 BSI 英國標準協會東北亞區 蒲樹盛（Peter Pu）總經理

年會首場講座由蒲總從宏觀角度談「營運持續與韌性全球趨勢」：從技術或者環境發展，資安早已不只是資安，該如何用全盤性思維提升資訊安全？就從「資安韌性」（Cyber Resilience）開啟。BSI 認為「資安韌性」屬於「組織韌性」（Organizational Resilience）的一環，企業保護資訊安全，從「資安管理」進入到「資安治理」：高層要負起責任，有能力參與資安策略訂定，確認資源支持執行；擅用國際標準做自身規範管理，落實日常管理；從法遵面提升資安治理[2]，視資安為組織營運與繁盛永續的核心條件，而使組織逐步具備「資安韌性」。

就世界經濟論壇（World Economic Forum, WEF）「2020 全球風險報告」指出的營運風險排名，網路攻擊（Cyber Attack）僅次於氣候暖化。2020 年網路攻擊較往年同時間數量升高 45%，主因是疫情導致數位化加劇與在家工作（Work From Home），假裝成公司內部或科技系統大廠的釣魚郵件頻頻出現，只要有任一成員受騙上當，整個組織隨之瓦解。要增加資安韌性，可從以下幾個面向著手：1.日常管理：牽涉到組織治理，高層要能支持資安管理在日常的組織作業流程中執行；2.風險管理：包含供應鏈與資產管理，尤其當供應商提供的設備或數位軟體來自高風險國家，是否有能力辨識與排除；3.保護力：針對網路攻擊，由被動防護提升至主動偵測；4.復原力：二十年前告訴台灣產業要有避風港（Back of Site）計畫，大家覺得這是非必要的投資，今日所有使用資訊服務的企業，備份已是基本動作。2020 年 10 月 1 日東京證交所發生停業一日事件，導因於備份系統過去五年沒有開啟，系統演練若無法成為日常管理的一環，形同虛設。企業組織可藉國家資通訊安全發展方案內的公務機關「資安治理成熟度」[3]自評，做為資安韌性的參考，知道自己的位置在哪裡──蒲總勉勵：「不要浪費 Covid-19 這個危機，國際標準是最好的圖書館，讓我們從中獲取解決方案與智慧。」

▶ 點此下載講師簡報

---

[2] 特別以金融業為例，法務與科技分屬不同單位負責，需確保雙方具有相同的語言，如此，法遵長才可支援資安團隊，確保該團隊的作為符合法規要求。

[3] 企業想要提升資安治理成熟度，可參考行政院資安處的資安治理成熟度架構，從策略、管理、法遵等面向來著手。

專題演講 2【攻守之間】

自動化企業資安威脅量測與案例分享

主講人 奧義智慧科技 邱銘彰（Jeremy）創辦人

奧義智慧科技創辦人邱銘璋（Jeremy），帶來「企業資安威脅量測與評估管理方法」：分享自己對資安防禦的心得與面向—1.掌握駭客攻擊手法 2.了解資安產品與服務，以及用 3.資訊流與管理框架來承載前述紅隊及藍隊服務，透由這三面向來衡量駭客威脅（見圖一）。同樣的結構也被歸納應用在資安奧義鐵三角當中，Jeremy 將其分為攻擊、防禦和框架（見圖二），分享企業對資安威脅與應變能力進行量測、評估及管理的方法，瞭解如何將企業的資安威脅與需求可視化、具象化地納入管理，從根本改善企業資安體質。

〈圖一〉資安防禦三面向

〈圖二〉資安奧義鐵三角

Jeremy 開場說明，現下資安要面對駭客攻擊、員工忠誠度、資安意識不足，與供應商內建軟體等複雜因素，即使企業在資安投資較以往高，資安防護無法跟上是現實。技術管理上，資安防禦已不在「阻絕」而在「偵測」，從釣魚上鉤到實際發動勒索攻擊有時序存在，是資安團隊可以發揮作用的空間。

就提出的資安防禦管理架構，與「你無法管理你無法衡量的事物」邏輯下， Jeremy 介紹 MITRE ATT&CK 與 Sonil 防禦矩陣兩項工具，前者將無邊際的駭客攻擊收斂成 428 招，後者讓企業得以評估所擁有的防禦投資落點，檢視漏失或需補強之處為何，兩者加乘使資安得以聚焦畫出範圍，投資管理即可最佳化。資安思維強調：資安委外不代表責任委外，即使委託的資安團隊偵測到出問題的 IP，但其代表的意義只有組織內部的人能識別；不會用工具的不需要買，應該是多學習；評估資安能量，識別一個攻擊從發現到回復要花「企業本身+廠商 + 防毒軟體+資安團隊」 多少人力金錢與時間，所做過的資安投資是否能將這個成本收回。

Jeremy 定義：資安成本就是「從未知到已知（Unknow to Know）所花費的時間金錢人力的總和」，而企業要如何在資安做投資？總結如下：

1. 善用安全事件應變（Incident Response, IR）：將發生過的駭客攻擊做成調查報告，以此為基礎，讓紅隊演練同樣的攻擊測試企業的資安能量，演練結果傳遞給公司的 IT 服務團隊進行資源調配，讓資安團隊的工作更有效率，讓調查報告發揮最大值。

2. 資安是可被測量的：按前述做好準備，讓駭客攻擊刺激資安免疫系統，將威脅攻擊可視化，量測從攻擊到處理完成花多少資安成本，持續改善 IT 架構，使偵測有效花費時間具體縮短，達成資安投資目標。

▶ 點此下載講師簡報

專題演講 3【與時俱進】

國際標準發展下的資安策略與風險管理

主講人 BSI 英國標準協會 孫文良（Sunny Sun）客戶經理

BSI 客戶經理孫文良（Sunny Sun）講座主題為「國際標準發展下的資安策略與風險管理」 ，梳理產業資訊風險、法規因應與國際標準發展，打底出資訊韌性輪廓；就執行現況彙整十大面向問題與解決，及可協助的標準落實方法：

一、法規的解讀不一致：

利用風險評鑑，從風險識別與風險接受度判定組織執行方向。

二、由上到下的管理 / 執行能力問題：

找出人員不適任的點，透過訓練或資源提供協助，或指導學習方向；不同面向的人材應提供不同的能力發展訓練（不要流於形式）；也要小心劣幣驅逐良幣的狀況發生。

三、文化思考模式尚未轉換：

找出團隊核心價值，使成員認知與目標對齊；獎勵>懲罰，使犯錯主動舉報而非隱藏；利用資安成熟度等工具，檢視改善與缺失，使資安成效具象化。

四、高度運用供應商但掌握度不足：

供應商是協助而非主導；若供應商服務交付發生問題，請重新檢視自我監督的議題；向供應商的專家學習，請第三方公正單位進行供應商交付服務稽核。

五、變更管理形成變更處理：

確保所有變更皆能事先經過危害辨識及風險評估，並採取適當控制措施；如果變更管理流程只有核准與交付供應商執行，易淪為單純執行而不具管理形式；特別要找出無授權的變更，實施管理。

六、未能找出有效問題根因：

根因分析要找到真正的起因點才能對症下藥；可利用過往事件練習根因分析的技巧；標準落實是要找出不符合的原因並採取行動，不僅是解決現況，更要確保在其他地方與未來都再不發生。

七、被動回應處理成本高於主動防禦策略

預防勝於治療；檢視組織在事故發生後所採取之控制，利用偵測找出預防面向；衝擊高而發生率低可考慮做風險轉移（像資安保險）。

八、未能有效合作展現團隊成效：

打破位階高低之分，訂定共同目標，分工而合作，共享成果；藉國際標準制定管理框架，定義配置責任。

九、資源投入未能最適化：

重新檢視（請專業協助）擁有資安防護機制、設備所具備的能力與使用程度，以發揮最大效益；人是組織的重要資源，人員能力是產生其他資源最適化的關鍵；標準強調識別組織資產，並定義適切的保護責任。

十、人員能力與實質獲得不等

勿用相同思考對應不同等級的專業人才；鼓勵並重視人才培養，支持成長空間；換用「若管理有效，就不用另外花錢」來思考人事支出。

Sunny 總結：從上述十個面向檢視組織體質，全盤了解狀況，對症下藥；團隊有共識與共同目標，始能有效運作；盤點識別手上資源並高效能運用，改善體質有效提升成熟度，不要讓所做的設置努力流於形式，使標準精神與法規意涵落實執行。

▶ 點此下載講師簡報

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）

「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。

眾所期待的「資安管理大劇場」，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。（更多內容詳 Part 2：綜合座談）

十幾年來 BSI 辦理資安年會，推動資安所費的時間和心力如同養大一個孩子，BSI 期許藉由年會，每年都能為台灣帶來前瞻性思維與國際間最新訊息；隆重的表揚典禮，是 BSI 給予年度提升資安體質、達到資安治理，朝資安韌性邁進的企業最真誠的肯定。

與會者趁年會議程休息時間，向工作人員洽詢 BSI 訓練課程。

看見所有獲獎企業皆深感榮幸，並緊握獎杯在獲獎單位介紹展示版前留下珍貴的合影紀念，以及到活動最後，現場座位人數一如開場，皆為年會籌辦團隊得得以全心投入，並年年超越最大的動力。

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 2：綜合座談〉

- **洽詢 BSI** ｜ 稽核驗證、產品測試、BSI 訓練學苑、VerifEye 認證平台、BSOL 標準資料庫