Part 1：會後報導

別幫駭客開後門─資安法下的「風險預測」及「防禦提煉」時代

2019 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

第十六屆 BSI 國際風險管理年會於 2019 年 11 月 22 日舉行。本屆主題聚焦於「資安法下的『風險預測』及『防禦提煉』時代」，道盡時下面對的挑戰與處境。本文將最新一屆的國際資安標準管理年會內容重點呈現，承載著這份基礎與展望，一同開啟 2020 年。

行政院資通安全處簡宏偉處長擔任開幕貴賓上台，簡處長從處裡的第一張資訊安全管理系統（ISMS）證書就是由 BSI 驗證通過的緣由說起，對資安「管理才是關鍵」感觸很深：隨著《資通安全管理法》（後簡稱資安法）上路，未來公務機關核心單位的 ISMS 三年內要通過第三方公正單位驗證，也希望將輔導與驗證切分開來。

行政院資通安全處簡宏偉處長站起來和全場的與會來賓打招呼，簡處長也是本次年會的開場致辭嘉賓，從資通安全處第一張 ISMS 證書就是由 BSI 驗證通過的緣由說起。

BSI 東北亞區總經理，也是台灣在國際上頗富盛名的資安專家蒲樹盛（Peter Pu）先生，以主辦人的身份歡迎現場所有與會貴賓與朋友，感性致詞：2003 年，BS 7799（國際標準 ISO 27001 資訊安全管理系統的前身）剛發布，BSI 台灣認為自己有責任要將國際上最新的標準資訊帶給台灣，讓台灣做好國際接軌，提升資安能力，於是辦了第一屆 BSI 國際資安標準管理年會。時至今日，道瓊永續指數（Dow Jones Sustainability Index, DJSI）評選新的指標要求有一半增加在資訊安全與個人隱私，資訊安全成為企業第一優先要準備好的挑戰，不分產業。資安法上路，公務機關、公營機構、八大關鍵基礎設施提供者或政府捐助之財團法人，相關規定如何遵守？同時看見資安人才的短缺，到處搶人才搶得厲害。本次年會並舉辦「資安管理劇場大探討」從策略、管理、技術與法遵四個面向，探討面對資安困境如何解套。最後感謝在場所有的優良企業組織及與會嘉賓，因為有大家的努力和參與，BSI 資安國際標準管理年會得以一直辦下去。

BSI Excellence Award 卓越組織表揚

每年資安年會，BSI 辦理資安卓越組織表揚典禮，十七年下來累積了近千家的資安優良組織，成為台灣資安環境的最佳動能，並從每年增設的獎項，看見時代演進。2019 資安卓越組織表揚典禮，新增獎項為：「資安人才培育獎」，受表揚的單位分別是 104 資訊科技與崴亞風險諮詢顧問。104 資訊科技，從早期大家對 104 耳熟能詳的：「替企業找人才」到現在「替企業培養人才」。而隨著主管機關對保經保代資安保險的重視[1]，有鑒於傳統保險業資安人才缺乏，以保險專業為基礎的崴亞風險諮詢顧問帶頭組織，從 2019 年五月起短短半年間，在台灣北中南辦了三十幾場資訊安全課程，保險從業人員參加踴躍，為企業資安保險險種鑑別核發，奠定人力資源。

擔任卓越組織受獎代表致詞的行政院國家資安會報技服中心吳啟文主任，幽默分享過去公務機關面對外部稽核時的特殊因應做法，強調資安是條漫漫長路，要秉著傳教士的精神，遵循 P.D.C.A 的步伐，將管理系統的文件內化成組織文化，才能真正降低資安風險。想必吳主任的心得，反映出所有卓越組織成員參與資安工作的心路歷程。

資安保護實踐獎（上圖）、雲端資安深耕獎（左下圖）、資安人才培育獎（右下圖）受獎代表與 BSI 台灣大家長 Peter Pu（上圖右四、下圖中）合影留念。

[1] 「108 年度公司治理評鑑指標」新增指標 2.24「公司是否建置資訊安全風險管理架構，訂定資訊安全政策及具體管理方案，並揭露於公司網站或年報」，將投保資安險納為評鑑加分項目。

熱烈而溫馨的表揚典禮告一段落，接著年會專題講座開跑，每場講座重點依序整理如下：

專題演講 1【國際網路安全標準發展趨勢 Outlook】

資安防禦提煉與個資保衛跨疆界

主講人 BSI 英國標準協會台灣分公司 謝君豪（Joe Hsieh）營運長

Joe 帶著招牌微笑，於本場講座帶來了三大重點：了解國際風險趨勢、分享台灣業界實況，以及國際標準最新發展。Joe 先從「5 大人物」[2]對人類全面生活影響切入，未來必定是資訊驅動業務，資訊人角色愈發重要談起，並從董事會（經營者）對資訊單位關注焦點，搭配世界經濟論壇（World Economic Forum, WEF）對各區域（東亞洲與泛太平洋、歐洲及美洲）所做的全球營運風險報告排名，資訊科技的風險節節攀升，網路安全儼然已是全球議題，資料外洩的威脅也榜上有名。再對應到實際營運管理，若資訊安全做得好，能協助彰顯企業在「環境、社會和公司治理」（Environmental, Social and Corporate Governance, ESG）上的成績，也是未來人才選擇企業的參考指標。

如何提升企業在資安組織管理的成熟度？**面對現實種種限制，Joe 提出「導入範圍不等於驗證範圍」的概念：將資訊安全從公司政策的高度請全體遵守，「全面要求，局部驗證」是很推薦的做法。各國際標準也提供很好的參考方向，協助企業按照內外部的威脅程度，決定驗證範圍的優先順序**[3]。回到國際標準，Joe 提醒大家用 ISO/IEC 27001 打底，用 NIST Cybersecurity Framework 網路安全框架做細緻度的優化。透過國際標準提升個人資料及隱私保護的成熟度，視需要結合採用 BS 10012、ISO/IEC 29100、ISO/IEC 29151、ISO/IEC 27018 等隱私保護標準建置並優化 PIMS 個人資訊管理系統；按全球趨勢需求所推出的 ISO/IEC 27701 隱私資訊管理標準也再次強調隱私議題的關鍵性；記得所有 ISO 27 開頭系列的國際標準系列，都是 ISO 27001 的補充包。Joe 最後提醒大家：「做資安不要為做而做，要符合目的和實用—有效比較重要」。▶點此下載講師簡報

專題演講 2【合規遵實踐】

《資通安全管理法》落實途徑

主講人 BSI 英國標準協會 孫文良（Sunny Sun）客戶經理

[2] 分別指：5G、大數據、AI、機器人和物聯網（IoT）

[3] 此處 Joe 建議鑑別關鍵業務流程—從機密性、完整性、可用性及法遵依循角度（S.I.P.O.C），訂定強化方向和優先順序，利用風險圖鑑，找出公司最關鍵的風險。

面對資安法的要求，有沒有好的方法和捷徑，不用靠自己摸索？Sunny 提出十個心法，從不同面向，按企業組織的需求，利用國際標準框架，找到對應落實的途徑。心法背後有很好的思維邏輯：**面對法規限制與其感到痛苦或逃避，不如借力使力，按照法規面的要求，檢視組織所處的位置、資安的成熟度，藉此訂定出策略，對應營運目標，用國際標準找到最合適的方式，跟著資安法逐步完成。**

可協助落實資安法的國際標準框架重點介紹：ISO 31000 協助企業做好風險鑑別；NIST Cybersecurity Framework V1.1 兼顧業務目標和隱私保護；COBIT 5 使用資訊技術，將 IT 治理與控制利益最大化；NIST SP-800-53 Revision 4 來自美國聯邦資訊系統和安全組織的隱私控制，Sunny 都建議拿來當參考書看，是可以免費下載的文件。BS 31111:2018 Cyber risk and resilience 則是高階主管做資安風險決策時很好的 Guideline。[4] Sunny 並提醒大家：如果發現導入了這麼多系統和檢測，還是發生資安事件，請您從組織文化切入改善，還有，資安通報事件執行效能關鍵在於獎勵大於懲罰。記得建立良好的資安環境，人才的培育，情資的分享，都是降低風險，為自己和整體共好能做的事。▶ 點此下載講師簡報

專題演講 3【經驗分享】

被低估的風險評鑑

主講人 DEVCORE 戴夫寇爾 翁浩正（Allen）執行長

Allen 以紅隊演練的經驗來分享，點出國內組織資安體質及防禦策略的盲點。最理想的情況，基於資安意識啟動，在重要性與成本的考量之下，訂定出企業的資安策略，並有效控制降低風險的成果，又回饋到資安意識本身，處於正循環狀態。Allen 指出，實際情況都是資安事件發生才驅動去想因應措施，缺乏策略，短暫因應只為了「下次不要發生」，無法達成正循環模式。駭客並非想像中散佈在各處的單一電腦高手，黑色產業已然成形，利用竊取資料勒索販售獲利。**唯有讓駭客竊取資料的成本大過於利潤，得以終止被駭客攻擊。**

單靠傳統的風險評鑑因應資安挑戰可能不太夠了，需要**用更技術的方式找出真實的資安風險是什麼。Allen 將資訊安全分成 5 個層次：真實的安全、潛在攻擊者的威脅、過去事件驗證過的安全、設備及系統安全、組織管理及維運安全**，依安全層次，分析各種測試方法優劣：針對組織管理與維護，導入管理系統標準化容易實作，適合組織起步遵循，但不易反映真實威脅；要測試出真實安全，可透過紅隊演練，最大化反映出可能問題（硬體設備、人員疏失、管理制度），找出潛在攻擊威脅，針對特定攻擊類型選擇因應措施，可節省成本，但缺點是發現問題過廣，沒辦法提供一次到位的解決途徑，或

[4] 請參閱第 185 期 BSI 電子報文章〈用標準找到資通安全管理法的落實路徑〉，孫文良經理演講內容。

不易辨識出攻擊者族群及手法。總結歸納：「真實性」是資安領域中很重要的一個主題，組織要從資訊安全 5 個層次由上而下，由下而上，不斷的修正，才能制定正確的防禦策略及風險評估；了解攻擊者技巧，以攻擊的角度補強資安策略，才能選擇合適的控制措施；針對持續出現組織中的攻擊技巧優先投入資源；以「路徑式」作為驗證資安策略的有效性，而非「單點式」。 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：行政院國家資安會報技服中心 吳啟文主任、iThome 吳其勳總編輯、 DEVCORE 戴夫寇爾 翁浩正（Allen）執行長、BSI 英國標準協會台灣分公司 謝君豪（Joe Hsieh）營運長

「資安管理劇場大探討」，左起：BSI 台灣營運長 Joe、DEVCORE 執行長 Allen、技服中心主任吳啟文、iThome 總編輯吳其勳 ，以及 BSI 東北亞區總經理 Peter。

「你的情境，我的借鏡」是本次資安管理劇場大探討的中心概念與用意，主持人 Peter 妙語如珠介紹各位與談貴賓。待大家在台上一字排開坐好，螢幕上一個個題目出現，主持人 Peter 用白話替大家直搗核心，聚焦在產業當務之急，並指定在場專家回應。（更多內容詳 Part 2：綜合座談）

第十六屆 BSI 資安國際標準年會在此圓滿告一段落，活動結束後許多聽眾仍依依不捨，與台上的嘉賓致意，與 BSI 的講師請教。每一年都這樣收穫滿滿，如同 Peter 說的，我們會一直辦下去。

休息時間大家絡繹不絕到 BSI 訓練學苑攤位，完成問卷換小禮物。

（年會議題相關文章請見下頁延伸閱讀）

延伸閱讀：

- 〈別幫駭客開後門─資安法下的「風險預測」及「防禦提煉」時代─Part 2：綜合座談〉
- 【個資管理系列】ISO/IEC 27701 隱私保護國際標準 簡介、條款 5 和 6、條款 7 和 8
  本系列三篇專家文章介紹於 2019 年 8 月發布的 ISO/IEC 27701 隱私保護國際標準，它是第一個兼顧隱私保護和個資安全管理的 ISO 標準，其內容結構讓隱私資訊管理可以被視為現有 ISMS 資安管理系統要求和控制措施的擴展。...
- 〈用標準找到《資通安全管理法》的落實路徑〉
  BSI 精選四大標準─NIST CSF、COBIT、NIST SP 800-53 和 BS 31111，運用其框架的核心優點，補足多數組織已建立的 ISO 27001 資訊安全管理系統（ISMS）與資安法的差距。...
- 〈以 ISMS 整合管理國際標準與合規性〉
  本文剖析如何應用資訊安全管理系統（ISMS）來推動一套整合的作法來管理如 ISO/IEC 27001、PCI DSS 支付卡產業資料安全標準和隱私等安全標準與法令遵循的義務。...
- 〈資安新時代：提升 IT 人職場競爭力的 3 個祕訣〉
  BSI 專訪 104 人力銀行副總暨資安長陳啓昌（Bryan Chen），談資安人才三大競爭力：品牌力、行銷力、學習力。協助還在摸索或者蓄勢待發的 IT 人，檢視自身條件，找到學習地圖，在資安新時代站上一席之地。...

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	ISO 27701 隱私資訊管理系統 基礎課程 建置課程 稽核員轉換 主導稽核員課程	雲端服務資訊安全管理系統 Cloud 主導稽核員課程	ISO 20000 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 稽核員轉版課程	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
資通安全管理法 稽核課程	BS 10012 個人資訊管理系統 基礎課程 建置課程 主導稽核員課程	ISO 27017 & ISO 27018 建置課程		BSI 營運衝擊分析(BIA)課程	ISO 27799 健康醫療資安基礎課程
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	NIST 網路安全框架 建置課程			

課程詳情請洽 BSI 訓練學苑：
T: 02-26560333
E: training.taiwan@bsigroup.com

- **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