清晰聚焦 資安推手

BSI 台灣客戶經理暨資深講師孫文良專訪

孫文良（Sunny Sun）｜ BSI 台灣客戶經理暨資深講師

責任編輯 徐瑋琳　採訪撰文 鄭詠中　校正修訂 黃純郁

去年《資通安全管理法》正式上路，資安即國安政策落地，BSI 資安客戶經理暨資深講師孫文良（Sunny Sun），從稽核和教育訓練各方著手，用簡單概念和容易操作的方式使資訊安全於各行各業深入廣泛日常化，一如他多年來持續所為，做一名資安推手。

IT 技術到資安架構 自己打基底

Sunny 從事 IT 架構工作超過 18 年，是台灣整合 IT 基礎設施，與資訊安全知識技術經驗的先鋒人才；能協助客戶統整資安管理系統要求、進行機房設計，一同建置資安管理系統、持續進行風險管理流程及風險分析，維持企業安全的有效性。深厚內功養成，Sunny 說有其時代性：民國 89 年，網際網路在台灣興盛起始，只要是唸資訊資管資工相關科系學子投入職場都很好找到工作；當時無人談資安，但替台灣資訊產業打下很好的基礎，完成台灣第一波數位轉型，從紙本走向數位化。桌上型電腦盛行，桌機網路設備伺服器，得靠自己在桌子底下摸索打理，於是墊起功力，至今台灣好些同世代出生的產業老闆，都有這樣的本領。

若要把世界數位化歷程做個分水嶺，的確 2000-2010 年，只要有網頁帳號密碼得以運作生意，先求生存下來，沒在顧及資安，台灣或全世界都是。只是 BS 7799（ISO 27001 資訊安全管理系統的前身），在這數位發展黃金前十年中段來到台灣，Sunny 有了資安啟蒙，上過 BSI 的資安稽核課程，沒有驗證已有思維，替服務的企業做資訊規劃，會把 ISO 27001 為母體，再把架構在控制項目上做設計，做出來的系統一開始就符合國際標準，之後再做轉型或驗證就輕鬆很多。

後來於企業內負責做 ISO 27001 系統導入，也是在資安驗證拓荒年代，無參考之下憑自己寫出第一份政策，從 IT 技術到資安導入，Sunny 馬步蹲得紮實。2010 年至今，世界資安發展期，前期 Sunny 累下的實力發功，利用下班與假日授課，接觸到的人開始多樣，Sunny 感受自己可以提供幫助，即使百廢待舉，依舊熱忱執行，小至企業大至社會，願做資安推手：「如果連我們都放手了，誰來做這一塊？」Sunny 說。

透過稽核 全盤清楚再向前

從 IT 技術到資安架構，Sunny 隨時代演進，打下厚實的基底，並清晰看見可以提供協助的角色。

「能幫到更多人」的概念支持 Sunny 離開服務已久的品牌企業，成為 BSI 稽核員。稽核工作不在告訴客戶該怎麼做，而是經過驗證，得以讓組織企業全盤清楚組織的狀況。「標準講的是 P.D.C.A，不是零跟一，沒有要一次到位。」Sunny 表示，組織可以從 60 分開始往上走，如同資安法裡面提到的「治理成熟度」，**透過稽核，讓客戶了解自己自己的最弱項在哪，強項就不用再花預算去提升了，知道風險為何，再看組織企業如何處理，至少不會處在一個迷惘的狀態，方向清楚，錢就能花在刀口上。**Sunny 再提國際風險在資安預測，實際發生時，預測第一二名風險項目的衝擊度反到沒有預期得大，因為組織企業有就風險評估針對最弱項去做因應，於是事件發生時，原預定最大衝擊得以減弱—當企業組織認為資源有限，無力全面改善資安條件時，更要請稽核專業做好風險評估，才得以讓預算發揮最大價值。

資安法上路超過一年，基本上產業依法該通過驗證的都做了。資安法沒有直接將供應商納入管轄範圍，但要求組織單位盡監督供應商之責，反而促進供應商主動想做驗證的需求：試想每個供應商有一二十家客戶，若每家客戶都前來監督，一定十分困擾，也會造成不同客戶間商業資訊外流的風險；另外，客戶派來進行監督的人員，不一定具稽核專業手法與技巧，是否真能稽核到位也有討論空間。直接請第三方公正單位進行最專業的稽核，通過驗證取得有 Credit 的證書，足以說明一切。**時下國內與國際具規模的標案，通過驗證往往是基本附加條件，從取得競爭門票的角度，供應商通過國際標準驗證是必備功課。**

資安法落實現狀

Sunny 表示，任何推動一定要有法遵循才能依法有據，當然任何法令在剛推出的時候一定無法盡善盡美，看資安法實施超過一年了，法條有寫到的基本上大家都有做到，但離納入組織文化還有一段距離，至少把底墊高了。Sunny 特別提到，風氣上最明顯的是通報由獎勵取代懲罰：過去事件發現者往往也是事件引起者，因操作意外事件發生，但因害怕被處罰而不通報甚至將痕跡抹去，會引發更多後續失控的風險。現在有少數企業具體明定：若通報查核屬實，則發獎金作為實質獎勵，但多數還是以懲罰為主。Sunny 強調做資安必須拉到組

織文化而非單點進行才會全面，而資安架構設計一定要讓執行者方便執行，並讓執行者了解自己在做的事情是有價值的，建立信心而願意多做一些。技術底出身的 Sunny，十分同理這些夥伴們的辛苦。

也因此，Sunny 看見實施資安法後暫時無法解決的現象：按資安法要求人員的配置，由於時間要求與資安人才短缺，於是可能未能選擇合適有能力的人員對應相對位置，運行時間久了一定會對組織產生管理與執行風險。Sunny 指出，學界或剛畢業沒有足夠經驗者，不適合直接承擔重要管理工作責任，因為不夠了解組織文化就執行資安工作會造成有效性問題。風險在人而非法律，Sunny 說，人才培養是長期工作，除政府主管機關政策性實施外，各組織需要重新重視經營人才培育的管理工作，目前普偏反應資安人才不足，反映出過往對資安人才疏於培養。而在新法實施一陣子後，必定就各行各業實施情況做意見歸納，將法條修得更貼近需求。Sunny 曾任主管，對人才運用別具心得，資安管理是需要不斷精持的課題，資安人才自身也需要不斷的持續精進，期待資安人可接受到該有的重視，做最適切的發揮。

訓練課程之必要與設計

雖然備課要花的時間和心力很多，Sunny 在在強調訓練課程之必要。做資安規劃多是運用在資訊系統上，如果資訊系統熟悉度不足，就會出現與相關人員雞同鴨講的窘境：「這就是為什麼要做訓練，讓每個人的素質達到相同水平得以溝通的程度。」有了共用的語言，效率才會顯現出來。Sunny 猶記得早期企業內對資安的認知薄弱，也無專責資安職務，相關作業都直接由系統人員執行，光聽組織業務人員提出需求，按自己的想像去執行，設計出來較難完整考量到資安面向實際所需：「**現在，資安人扮演中間溝通的角色，你可以不必親自去做，但你能夠幫業務需求經由資安思維轉化成系統用的語言；或許你不是實作的人，但你是在中間做溝通的人**」。

在課程設計上，Sunny 路線是淺顯易懂，並自我要求：「能否用一張圖去呈現出整個架構邏輯，效果就強過很多文字敘述。」要做出來一定得花很多功夫去消化思考。Sunny 明白很多學員付錢來上課是為了考證照，但每一位學員的背景養成不一，Sunny 盡力做到讓所有學員在最短時間得到他們要的。老實說這個領域總會遇到覺得自己程度比大家都好的人，Sunny 會在課程開始前就將環境設定好，告訴所有學員：「在這裡沒有人問問題會被笑，我們就是要一起作戰，得到認證。」想幫助人的初衷，用同理體察人心，Sunny 把力氣精準花在每一次出擊上，訓練或者稽核皆是。

獨特的紓壓方式

連客戶都知道，Sunny 釋放壓力的方式就是考證照。平均一年一到二次，最多四次，都是國際證照。Sunny 解析：不是要證明什麼，能在自己專業領域中越精進了解，工作上也能越得心應手；資安領域的書已經看出興趣來，書讀得越多，讓腦袋越循環。

Sunny 從稽核從訓練等各方面著手，用簡單概念和容易操作的方式使資訊安全於各行各業深入廣泛日常化，持續所為，做一名資安推手。

稽核員就是一種「一但進入這個行業，就會有讀不完的書」的職業，Sunny 會不會太適合這個角色設定了。Sunny 說自己一但決定要考證照，會先刷卡報名，然後倒數計時知道自己還剩多少時間資源可以準備，訂出計畫按進度執行，然後考試通過取得證照，壓力解除得到成就，一氣呵成十分紓壓。當然，家人的支持是重要的，每到最後衝刺階段，感謝另一半將小孩帶出門活動，讓 Sunny 在最舒適自在的環境專心準備，成就了 Sunny 獨特的紓壓模式。

能成為 BSI 的稽核員都絕對優秀，也都勤奮，否則無法勝任。若說對 Sunny 深刻的印象，會說他清晰聚焦，聚焦在自己最適合的定位，如同調音師將自身整體狀態時時校準，演奏出最精確的旋律，傳遞給最需要的耳朵，使其獲得啟發與幫助。最後告訴大家一個小秘密：Sunny 穿得每一件襯衫都是由自己親手熨燙，每個星期日 Sunny 會留一小時在家燙襯衫—聰明之人皆有癖，下次遇到 Sunny，可以問他一個人燙衣服的時候都在想什麼。– 全文完 –

BSI Careers

- 更多 BSI 稽核老師的專訪內容請前往 BSI 官網閱讀
- 聯絡 BSI：infotaiwan@bsigroup.com | 02-26560333