全球資安事件頻傳的 2017 年，多項重要且急迫的資安議題受到高度關注，也讓「2017 BSI Standrds 國際標準管理年會」在開放報名後隨即爆滿。BSI 國際標準管理年會包含了卓越組織表揚典禮與論壇，辦理 20 多年來已成為國內企業組織獲取國際最新標準、管理方法、解決方案與實務對策的焦點盛會，BSI 今年提出「資安管理 4.0」的概念，安排多位專家用精闢且幽默的演講內容引導大家，從大家熟知且廣泛應用的 ISO/IEC 27001 資安管理系統開始延伸，串起過去的資安佈署，擴充未來的防禦策略。

資安管理關乎整個組織

行政院技術服務中心吳啟文主任開場致辭時表示，資安標準非常重要，能為資安推動的工作奠定良好的基礎並建立許多機制與 SOP，而能否落實，則是另一項重要的因素，從最近的資安事件可看出，許多都是因為有規定但未能落實才導致問題發生，因此行政院近期也著重推動資安稽核，更希望把資安管理提升到資安治理的層級。吳主任分享，過去在推動資安管理時，很多人都認為這是資訊部門的責任，但從目前的資安風險看來，資安管理應該是與整個組織有關係，是整個組織風險的一部分，組織的首長應該更加重視資安管理，並投入更多資源。

以組織韌性培養應變力 將是組織存活的關鍵

BSI 英國標準協會台灣分公司蒲樹盛總經理在論壇上說到：「科技」是不分職業、不分行業且不分教育程度的，企業組織如果要生存，就必需要跟上這些應用，但隱私跟安全的議題卻與科技應用如影隨形。蒲總經理藉由分享最近的 AI 電影、重大資安事件以及網路詐騙案例與手段，並對應到 2017 世界經濟論壇的全球風險報告，再從 2017 年由 BSI 與 BCI 英國營運持續協會所合作的調查報告中看到不謀而合的前 3 大營運中

斷威脅—網路攻擊、資料外洩、無預警的資訊與通訊中斷，引導大家審視並重視資安威脅的演變與挑戰，以及歐盟最新的 GDPR 一般資料保護法會對全球企業組織造成怎樣的衝擊。

蒲總經理說到，應變力很重要，歐盟近期開始提倡「組織韌性」的觀念，將過去我們用以評斷一家組織的產品、流程、願景、策略、財務、領導作為...等顯見的條件視為「營運韌性」，而藏於其後的「資訊韌性」與「供應鏈韌性」將是日後組織存活的關鍵，透過這 3 種韌性與相應的國際標準來培養應變力。

“被動回應已無法因應資安威脅，主動管理才是對策”

洪進福 副總工程師
中華電信數據通信分公司

議程一精華摘錄

“將法規要求化為控制措施，法遵人員與資訊部門需要多溝通”

吳晟熙 產品經理
BSI 英國標準協會

議程二精華摘錄

“資安管理的目標從來就不是 60 分，應以「遵循性」立基，築「有效性」而上”

謝君豪 協理
BSI 英國標準協會驗證部

議程三精華摘錄

【精華摘錄一】被動回應已無法因應資安威脅，主動管理才是對策


洪進福 副總工程師
中華電信數據通信分公司

新科技必定會帶來新的機會與挑戰，從金融 4.0、工業 4.0、物流 4.0、支付 4.0、零售 4.0、區塊鏈、FinTech...等不同行業領域的創新技術與應用實務發展來看，確實有許多的資安紛擾持續不斷，而它們的共通特質就是連網化。

中華電信數據通信分公司洪進福副總工程師在年會上揭露了許多 HiNet SOC 的獨家數據與觀察，分享了如：2016 年勒索軟體類型成長 7.5 倍，每日約 750 個企業或使用者遭到感染。DDoS 的最大攻擊規模為 111 Gbps，一般企業對外連線約數 Gbps，無需太大攻擊量即可癱瘓系統運作，其中又以 UDP Flooding 為大宗，而且攻擊對象偏重資訊通信業，其次為製造業、服務業、學術教育業、金融保險業...等。暗黑產業的也開始進化，藉由 APT 感染 IoT 或連網的閒置設備來發動攻擊，因此企業的資產盤點管理 (Inventory Management) 就非常重要。

洪副總工程師笑說：儘管許多企業都有制定管理制度，定期做社交工程演練，不過資訊安全被理解成是一種「衛生習慣」，內部同仁可能重覆誤觸相同的資安陷阱，需要長時間的持續引導。

目前資安環境急速變化，組織不能未考量外部資安議題，或只偏重內部資安議題，且應隨時掌握資安威脅情資、主動建立預警，調整防禦策略。洪副總工程師提醒來賓，既然外部威脅是無法左右的，企業可以做的就是管好自己的漏洞，避免暴露在外並適時的採取因應措施，也藉由衝擊分析讓高階管理者知道應該要投入多少資源改善，透過管理、防護、情資三管齊下才能以不變應萬變。

【精華摘錄二】將法規要求化為控制措施，法遵人員與資訊部門需要多溝通

從支付寶、歐付寶、微信...讓我們看到支付型態走向電子化，這不代表傳統的信用卡交易勢微，而是信用卡已朝向虛擬化卡號發展，在支付工具發展的過程中，資安風險與法令遵循的議題總是伴隨左右，也突顯了資訊單位過去被定位在支援單位，在作業上常面臨的困境是不懂法令法規的要求，也不清楚該遵循那些國際標準，若組織恰好有提供或執行信用卡相關服務，資訊單位同仁可能有聽過 PCI DSS 支付卡產業資料安全標準，但不一定知道規範詳細的要求，也不清楚這其實是個強制性的標準，就更不用談能在符合性之上達到多少有效性了。

至於要如何透過 ISO/IEC 27001 來面對新的法規要求，BSI 英國標準協會吳晟熙經理舉了簡單的例子：ISO/IEC 27001 是個框架，組織可以依照內外部各種要求的強度來決定實施管控的力道，但 ISO/IEC 27001 沒有明訂密碼的長度，金融業可能普遍要求 8 碼，電信業可能到 12 碼，究竟幾碼才是安全的，ISO/IEC 27001 無法告訴你答案，若能參考到自身產業所適用的其他法令法規，就有機會發現更明確的要求，並能應用在 ISMS 程序書的規範當中。就像 PCI DSS 標準內的 6 大目標及 12 項要求，幾乎都可以對應到 ISO/IEC 27001，若您的組織恰好有提供或執行信用卡相關服務，可將 ISO/IEC 27001 作為資安管理的原則，而將 PCI DSS 視為實際上要達成的程度。

吳經理建議企業組織在清楚辨識所面臨的法令法規並轉譯給資訊單位後，可以分別從管理面與技術面著手，管理面─應用 ISMS 框架收納各式資訊安全要求、組織內須具備熟悉資訊作業法規及資訊安全技術的專才、參考國際標準最佳實務建立資訊安全基準 (baseline)、Security / Privacy by design、強化組織員工的遵循意識 (包括業務單位及資訊單位)、依最小化原則處理支付資料，最後則是自評/內部稽核的有效性；技術面─實施資訊安全防護技術，IDS/IPS、WAF、弱點掃描、滲透測試、考量進階資訊安全防護技術、強化監視機制的實施有效性 (例如: 日誌審查)。

【精華摘錄三】資安管理的目標從來就不是 60 分，應以「遵循性」立基，築「有效性」而上

BSI 英國標準協會驗證部謝君豪協理表示，各界在從事資安工作時最容易遇到「策略、認知、管理、技術」這 4 大挑戰，而其中最重要的應該就屬「策略」了。過去稽核過許多單位都非常重視資安，但可惜的是範圍都受限在資訊部門，面對其他部門對資安的認知不足或配合度偏低，都成為看的到卻管不到的弱點。此外，資安特勤小組的位階是否夠高，權責是否清楚，如何在業務面的安全與便利性之間取得平衡，同樣是攸關資安工作推動能否成功的一大重點。

謝協理表示國際標準為了適應各行各業，在制定時所列的條件通常是採最低基本要求，但這不代表資安工作就該僅止於此。有些組織在導入管理系統時抱持著「多做多錯，少做少錯」的想法，將各種管控措施盡可能精簡，凡事採取只求 60 分的心態，的確有可能讓稽核順利過關，如此為了驗證而做驗證的消極態度，早已讓管理系統失去應有的作用。加上近幾年許多產業積極進行轉型，將原本的業務內容改造升級或創造出新的業務內容，政府機關也相繼推出 APP 或將公眾服務網路化，但既有資安規範常常無法滿足新創業務的基本需求，反而讓業務單位覺得窒礙難行，若未予以調整，其他單位甚至到最後就選擇不再配合，但他們真的有錯嗎？或是管理制度的「有效性」出了問題？相信是值得大家思考的議題。

除了來自管理制度面的挑戰外，拿不到預算也是資安部門常見的苦惱，這或許並非因為上級不重視資安，而是上級「看不到」有哪些該改善。謝協理認為要克服此點可先從展現資安管理的「成熟度」來著手，第 2 步是結合其他標準的風險管理機制，透過風險評鑑量化所面臨的資安風險以做必要優化。最後才是開始精進 ISO/IEC 27001 的控制措施，並參考其他國際標準與指引加以拓展。

謝協理提醒大家，資安管理的「有效性」一定是最重要的，但沒有做到遵循，也談不上有效，大家不應該為了資安而做資安，只有形式上的管控制度，也不願意呈現真實的資安現狀，未來恐怕就只能概括承受所有的資安風險了。