強化企業組織的資訊韌性(information resilience) 以提升整體資安管理的成熟度及綜效

撰文：BSI 台灣分公司驗證部協理
謝君豪（Joe Hsieh）

這幾年對企業組織的相關主管來說，感受一定越來越深刻，那就是企業組織內部資安控管的有效性越來越不易呈現了。主因除了全球數位化、新興科技的演變及應用、網際網路的高度使用外，虛擬貨幣（如：比特幣）的興起也讓駭客有了獲得財務收益的機會與途徑，促進暗黑市場的興盛並導致攻擊手法越來越多樣化。造就這個人在變，物在變，技術也在持續變的資安環境，想靠傳統的安控或資訊單位以不變應萬變，恐怕會連現狀都很難保住。

BSI 每年皆與全球多家研究機構合作進行研究調查，其中與英國 BCI 營運持續協會連續 6 年發行的地平線掃描報告中，不僅可觀察出因為全球數位化及新興科技所衍生的相關新興營運風險及對企業組織造成的衝擊，也能觀察到不同的風險是如何在各產業間交互影響的。綜觀此報告在 2017 年對各產業面臨的威脅、造成服務中斷的衝擊，以及未來趨勢的分析結果中可發現，即便是不同產業或國家，所面臨的前 3 大威脅幾乎都是「網路攻擊、資料外洩、資通訊的非預期中斷」，所鑑別出的未來趨勢也有高度的相似，如用網際網路進行惡意的攻擊，而上述這些風險都與資訊安全及網路安全脫離不了關係，更橫跨各個產業。身在全球數位化時代的企業組織們應該要更有自覺與意識，絕對不能為了資安而做資安，應該是為了風險而做資安。

謝君豪

台灣資安及稽核業界資深專家。在 IT 及資訊安全領域有超過 22 年的工作經驗，及超過 14 年的稽核經驗涵蓋 ICT、金融、高科技、製造業等。現任台灣科技化服務管理協會（ITSMA）理事、國家資通安全教育訓練講師，於 BSI 擔任驗證部協理、ISO 27001 與 ISO 20000 產品經理。具 ISO 27001、ISO 20000、ISO 9001 主導稽核員資格，及 ISO 27001、ISO 20000、BS 10012、CSA STAR 及雲端安全系列資深主任講師。

資安布局需要高度、廣度與深度，還要並重管理與技術

企業組織目前在進行資安的推動及管理時最常遭遇到「策略、認知、管理、技術」這 4 大面向的挑戰，而其中最關鍵的挑戰應該就屬「策略面」了，許多企業組織的管理階層都知道資安的重要性，也表達非常重視資安，但可惜的是對資安的認知範圍大多還都是侷限在資訊部門，在沒能通盤檢視且正確規劃之下，選擇局部的導入資訊安全管理系統（ISMS）及進行局部的驗證。儘管資訊部門的確是大部分企業組織的資安管理重點，但如果其他業務/行政部門對資安的認知或配合度偏低，成為看的到卻管不到的弱點。這種廣度不足的管控制度，將可能成為未來的資安未爆彈（社交攻擊就是一個很明顯的例子）。此外，「策略面」還包括資安推動相關權責的明確定義及授權，如：資安推行組織在企業組織內的位階是否夠高及能否提供足夠的資源及展現支持。在企業組織目前面臨到業務轉型時所遭遇到的安全與業務便利性間的重大衝突時（business and IT transformation），企業組織的管理階層的明確指導及支持將是攸關資安工作能否成功的一大重點。

另一項可能讓資安工作不易展現成效的是偏重單一面向的活動（如：偏重技術面但不重視管理面），舉例來說，資訊單位認為資安專職部門配有專業的資安技術人力，像資料庫管理員所執行的各項活動後所產出的系統日誌理應由相關的資安同仁負責檢視，但資安專職部門的看法可能則不盡相同，認為資安同仁並無法了解所有的作業內容或是具備各種資料庫管理的高度專業能力，不可能有能力檢視所有類型的系統日誌，如此一來系統日誌的審查即有可能變成了三不管地帶。

國際標準是資安的底線（baseline），企業不該自我侷限

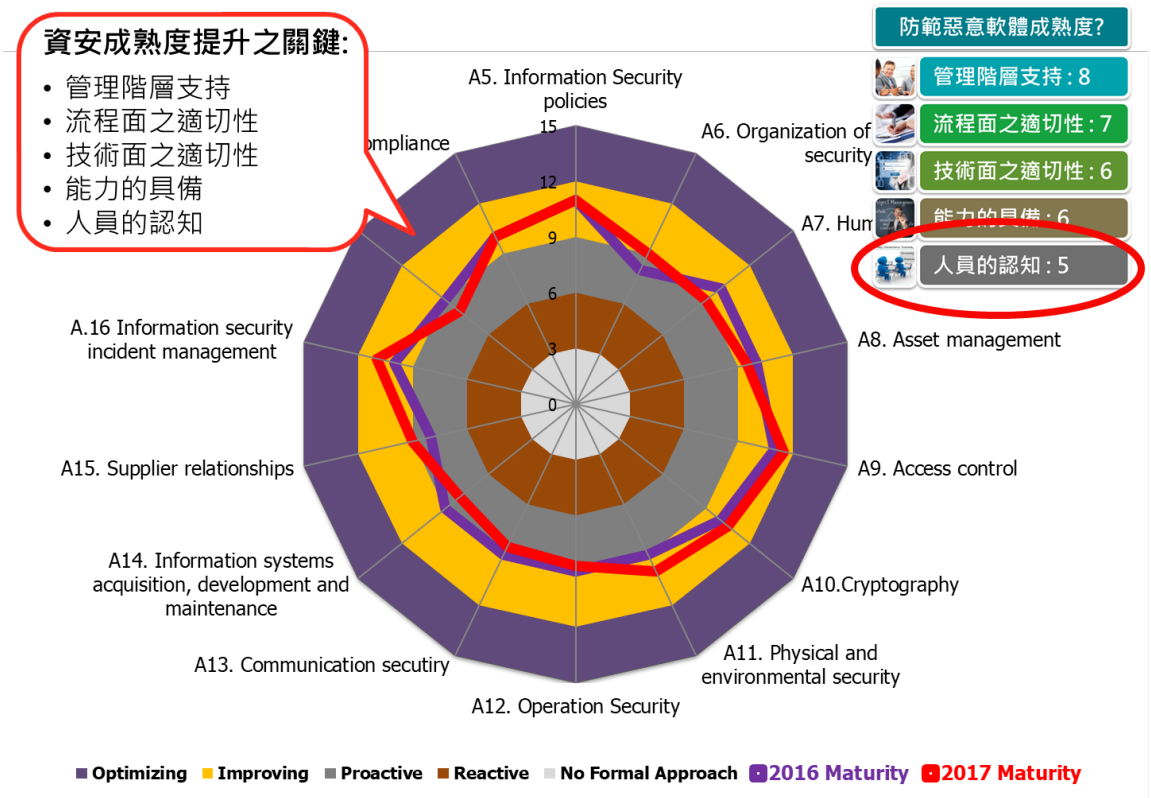
國際標準一般來說都是共通性的標準，也就是為了讓各行各業可以遵循，所以在標準中所訂出的要求都是共通性的要求（也就是企業組織該遵守的 baseline），但這不代表資安工作就該僅止於此。有些企業組織在導入管理系統時抱持著「多做多錯，少做少錯，不做不錯」的想法，將各種管控措施盡可能精簡，凡事採取只求 60 分及格的心態。加上近幾年許多產業積極進行轉型，將原本的業務內容改造升級或創造出新的業務內容（business transformation），但現有的資安規範與程序書常常無法滿足新創業務的基本需求，反而讓業務單位或負責的單位覺得窒礙難行，若未予以調整，部分單位甚至到最後就選擇不再配合，但他們真的有錯嗎？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。

以「成熟度模型」合理的展現績效並量化資安弱點、提升安控措施的有效性

資源不足常常是目前很多企業組織在推動資安時所面臨到的挑戰之一，這或許並非

因為管理階層不重視或不願意提供，而可能是因為權責部門無法有效的具體展現出資安目前推動的成效及面臨到的關鍵議題，管理階層在無法「看到」有哪些活動或議題真的會影響到企業組織的運作，自然不容易再給予更充分的資源。如果企業組織在推動時可以透過適當的機制及作法展現出資安管理的「成熟度」，並讓管理階層瞭解到企業組織當前的資安管理制度或資源有優異之處，但也有「相對」不足的地方需要優化，管理階層勢必更清楚須提供必要資源以因應相關的風險。那可以如何展現呢？

第一步就是先透過適當的方法呈現目前的資安成熟度以供管理階層了解，以 BSI 在進行稽核時為客戶所提供的**資安成熟度分析**為例（BSI 的資安成熟度模型共分為 5 個層級──第一級「無正式方法」、第二級「被動」、第三級「主動」、第四級「改善」、第五級「最佳化」），此成熟度模型不僅可提供給企業組織作為目前資安管理制度是否完善的參考依據，企業組織也可以透過成熟度模型逐年進行自我比較，找出不同階段應精進的目標方向。



圖：BSI 的成熟度分析模型

下一步則是可將資安管理結合內控、個資、BCM、ISO/IEC 20000 等其他標準中的風險管理做法，以整合式的風險評鑑方法鑑別出企業組織所面臨到的各類風險，以避免疊床架屋並重複投入資源。企業組織可參考 ISO 31000 風險管理國際標準的原則與準則（目前新版正在修訂中），所鑑別出的風險才夠真實、務實且具邏輯性，再加上對資

安成熟度的精準掌握，才可能讓管理階層了解所面臨的實際風險並投入資源補強。

最後可考慮開始精進 ISO/IEC 27001 的控制措施，並參考其他國際標準與指引加以拓展，以網路攻擊此項風險為例，組織可以更進一步瞭解網路安全事件應變（Incident Respondence）、軟體開發安全（Coding Security）、營運持續管理（Business Continuity Management）...等相關的標準以在 ISO/IEC 27001 的基礎上進行拓展。

法令法規跨國界，GDPR 率先衝擊全球企業

除了網路安全外，歐盟一般資料保護規範 GDPR 可說是近期最熱門的資安話題之一，特別是新興科技發展所衍生的某些個人資訊資料，像 Cookie、IP 位置、GPS 定位...等，也都是納管的對象，GDPR 不僅僅是個人資料保護，還牽涉到網路安全、資訊供應鏈、IoT...等各領域和產業的議題，在這早已打破疆土邊界的網路世界裡，相信很少有人能置身事外，但該如何因應？

由於 ISO/IEC 27001 僅提及組織應遵循相關適用法令法規的要求，確保隱私權及個人識別資訊的保護，但並未有針對性的作法，相關的個人資料保護風險可能無法被突顯，因此上一段文章強調的「延伸」觀念就派上用場了，組織面對越趨嚴謹的歐盟個資法規，可以**參考 BS 10012 個人資料保護標準的管控措施來證明已符合 GDPR 的要求**。

BS 10012 在今年初改版並導入 GDPR 歐盟一般資料保護規範的觀念，對於提供支付卡服務、旅遊業者、電子商務、高科技製造業、在歐盟有企業分點，或是其他商務應用而可能處理到歐洲居民資料的組織來說格外重要，先前提到驗證用的標準通常僅列基本要求。如您是上述對個人資料保護有高度需求的企業組織，還可以透過 ISO 29134 來做隱私權衝擊分析，或用 ISO 29151 來做個人可識別/隱私資訊的保護，此標準從 ISO/IEC 27001 裡 114 個控制措施中鑑別出 36 個做額外的補強；若想要知道組織在隱私保護的能量是否足夠，就可以參考 ISO 29190 做能力模型。在這國際接軌的時代，確保隱私資料被妥善的保護，絕對是組織必要的責任與義務，各界應該要多加應用 BS 10012，展現企業組織善已盡良善管理之責。

資安管理的目標從來就不是 60 分

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。

● **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

BSI英國標準協會

T: +886 2 2656 0333 ｜ E: infotaiwan@bsigroup.com ｜ www.bsigroup.tw