面對混合式資安風險管理挑戰

對所有組織來說，如何有效因應組織因營運業務變化所面臨的風險及挑戰，已是刻不容緩的議題，尤其資訊安全的有效管理與否，更是重大考驗

全球化及數位化的大浪潮下，組織現在面臨的競爭已早由同業競爭轉變成異業競爭，既有的傳統營運及獲利模式都被顛覆。

以金融產業為例，現在最大的競爭挑戰可能是 FinTech 業者（可以試想 Google、Facebook、Apple 等業者，在其全球超過數 10 億用戶所使用的服務中，要加入一個新的金融交易服務功能，應不是難事）。

對電信產業來說，最大的競爭對手可能是 Apple、Skype、Line 等服務提供者，使用者不用再付費，就可使用簡訊、通信等服務。因此，許多組織現在都面臨到一個關鍵挑戰：那就是要快速地推動業務創新及轉型，業務導向的趨勢將不可避免（服務上線速度要快、品質要好、服務要即時、功能要完整，但僅有很短的時間進行規劃及建置）。

加上許多新興科技或服務的衍生，如：IoT、Big data、Cloud、Mobile service……等，組織的同仁對新技術的掌握程度越來越低，僅能大量依賴解決方案供應商進行建置及維運管理活動。在這狀況下，要不發生資安事件或故障的難度及挑戰，就越來越高了。

資訊安全是威脅組織運作的重大因素

在 BSI 英國標準協會，以及 BCI 營運持續協會（Business Continuity Institute）於 2016 年所進行的全球營運威脅調查當中，特別分析出全球各個地域會造成組織營運無法持續運作的前三大關鍵威脅，以及未來的前三大發展趨勢，而我們從中可以發現幾個重點，那就是，全球的組織都同意最關鍵的前三大營運威脅，都與資訊安全議題脫離不了關係（網路攻擊、資料外洩、非預期的資訊與通信服務中斷），尤其以網路攻擊（Cyber Attack）在全球各地，都被視為最關鍵的安全威脅及風險。

像是勒索軟體（Ransomware、零時差漏洞的攻擊、新型態網路社交工程詐騙、APT、DDoS……等），一旦未能有效預防、監控甚至是即時應變，造成的影響及衝擊，對組織來說，可能是無法想像的。像 2013 年美國的 Target，其支付系統被駭客入侵，以及 Sony 的 PSN 服務被駭客入侵，都造成這兩個組織在財物及形象的重大衝擊。

因此，組織要如何在整體環境的急遽改變下，在創新、競爭力、法規遵循、客戶資料保護、服務品質，以及資訊安全等層面，取得平衡點，一定是未來的管理重點。

以現在受到高度關注的 FinTech 為例，不管從世界經濟論壇或是臺灣金融主管機關所發布的金融科技發展策略白皮書中，都可發現：網路支付、P2P 網路放貸、機器人理財、大數據核保理

謝君豪

BSI 英國標準協會驗證部協理，現任台灣科技化服務管理協會（ITSMA）理事，於 BSI 擔任 ISO 27001 與 ISO 20000 產品經理。在 IT 及資安超過 22 年工作經驗，超過 14 年稽核經驗，涵蓋 ICT、金融、高科技、製造業。

BSI 與 BCI 於 2016 年進行了全球營運威脅調查，圖中為該份報告所分析的前三大營運威脅（以白色標示），以及未來的前三大發展趨勢（以黃色標示）。

賠、大數據信用分析、區塊鏈技術……等，一定是未來的發展趨勢，且未來對金融產業及周邊相關服務提供產業都會造成影響（如：銀行、保險、證券、電信、資訊服務提供者、平臺服務提供者……等）。

在組織因應未來的業務及營運轉型及挑戰時，如未能妥善規畫及制定未來的「轉型計畫」，可能將會無法有效因應相關的風險。

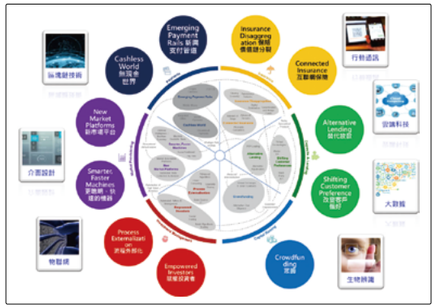
這也是許多組織的資訊部門，現在所面臨的情況——該如何建立合適的 Bimodal IT 的服務模式（也就是所謂的傳統 IT 與快速 IT 要同時運行），且需要因應相關的業務特性，量身訂作所需要遵循的資安控管規範。同時，這也是目前很多組織高度困擾的問題——如何在安全及快速、品質，取得平衡點。

用 4 個 P 強化防護，增加組織面對資安威脅挑戰的韌性

筆者認為，要有效地因應未來面臨的資安挑戰，組織必須要能夠在策略、管理、技術，以及人員等四個面向，進行加強（或是簡稱為 4 個 P，即 Process, People, Product, Partnership），以提升整體的資安防護能力。

舉例來說，如果組織處在資安已是高度複雜的環境中，但仍在遵循好幾年前制訂的安控管理規範（outdated），或是因資源關係，大量的新服務均由解決方案供應商來建置及維運，組織內部資訊人員完全沒有能力監督及管理……等，卻希望不發生資安、個資、ICT outage 的議題，其實是非常難避免的。

這時，組織本身應該要建立及提升所謂的「組織韌性（Organization Resilience）」的能力——也就是，能夠預測、準備、應對、適應環境的持續變化，以及突發性的營運中斷，讓組織能繼續生存和發展的能力。



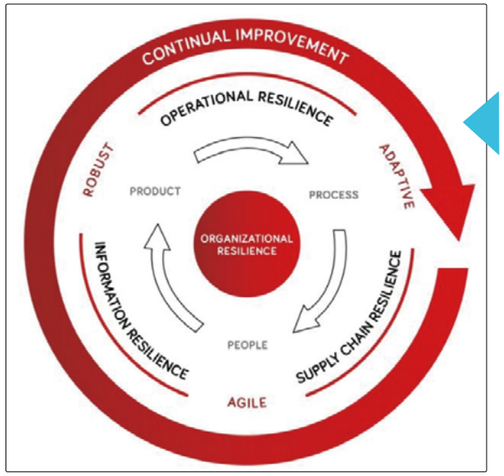
在 2015 年世界經濟論壇當中，針對金融服務的未來發展，提出了 7 大功能，以及 11 組創新。

從近期國內外發生的重大事件來看，如：臺灣機場淹水、三星新手機重大瑕疵召回、美國摩根大通被入侵，8 千多萬客戶資料遭竊、美國 Target 內部因為忽略潛在的資安通報，造成超過 1.1 億筆客戶資料外洩，都在在顯示其重要性。

根據經濟學人智庫在 2015 年為 BSI 所做的一份全球研究顯示，88% 的組織認為，提升組織韌性能力，以確保組織能夠長期存續，是其營運優先要務之一。但在調查中，僅有三分之一（29%）的組織認為，他們已具備良好的因應及復原能力，預期在三年之內可具備相關能力的，則不到一半（44%）。

此外，在上述分析中，也鑑別出建立完善的資訊安全管理，同樣是確保組織韌性的重要因子之一。由 BSI 所制定的 BS 65000 組織韌性指引標準，提供了一個非常明確的指引框架：要建立及提升組織韌性，必須從三個面向進行強化：營運韌性（Operation Resilience）、資訊韌性（Information Resilience），以及供應鏈韌性（Supply Chain Resilience）。

其中的資訊韌性面向能否有效提升，與組織能否有效地針對營運活動相關的安全進行管理，有著密不可分的關係。因此，為了要能夠有效的因應未來急遽變化的業務轉型，以及新形態的資安攻擊與風險，組織可以參考國際標準的要求，先在管理面進行必要的強化，再依實際需要在技術面及人員面，進行必要的提升。



BSI提出的組織韌性，包含三大重要領域：營運韌性（Operation Resilience）、資訊韌性（Information Resilience）、供應鏈韌性（Supply Chain Resilience）。

遵循性不等於有效性

此外，組織也必須建立正確觀念：管理制度的導入最強調的部分是「有效性」，而不僅僅是「遵循性」。

舉例來說，組織依照標準的要求，訂定了 BCM 的規範（營運持續管理）及 BCP（營運持續計畫），也定時依照規範進行演練及檢討，這樣可以說是達到了「遵循性」的要求。

但是，在 BCP 中所考慮的情境或是嚴謹度，並不夠周延（例如，僅考慮到部分情境，如火災、地震；而嚴謹度或涵蓋度不足，例如，天然災害設定的情境，沒有盡量考慮到較嚴肅的狀況，導致啟動 BCP 時，仍無法因應），而這是「有效性」不足的議題。

近期筆者看到好幾個組織，其資安的控管規範已是幾年前訂定的要求，但組織的營運及職掌早就產生了很大的變化，這樣很難確保資安能夠有效被管理及監督。

以更大的格局來思考

為了能夠有效強化組織的資訊韌性（Information Resilience）與能力，其實，組織可考慮以全局的角度，鑑別組織目前及未來的營運發展策略，進行管理系統的整合導入，以強化整體管理的綜效。

舉例來說，組織未來希望在第三方支付業務進行發展，這時，就可考慮整合 ISO/IEC 27001、PCI-DSS、Data Protection 的要求及精神，進行內部管理制度的強化。

以風險管理為核心概念的資訊韌性。

如果組織面臨到業務的轉型，需要同時提供傳統的系統開發模式，以及新創服務的開發服務模式（如：Agile），那麼，可考慮以 ISO/IEC 27001 為基礎，並透過其他的做法，像是：SSDLC（Secure SDLC）的指引，進行 Bimodal IT 開發的服務模式規畫。

整體而言，資訊安全已是組織日常維運無法忽略的議題，不論是從政府主管機關要求、法令法規、客戶要求，或是自身要求等面向，未來，對於資訊安全治理的要求，一定會愈趨嚴謹。

組織也必須正視相關資訊安全威脅趨勢的變化，而造成的潛在衝擊，以及挑戰（如：透過 Internet 進行惡意的攻擊），進行必要的管理能力提升。

許多組織在推動資安時，常在管理面及技術面中間掙扎，不知該先以哪個面向進行強化。依照筆者過去的稽核經驗及國內外資安事故的分析，許多資安事故的發生，都與人員落實度不足及便宜行事有關。

航空界有個不飛行安全的理論，稱為海恩法則：每個嚴重航空事故的背後，必定有 29 次輕微事故、300 個瀕臨事故徵兆，以及超過 1000 個潛在問題。而在資訊安全的管理，也是雷同的觀念，如果先透過國際標準及相關指引的要求，進行制度的訂定，再透過技術面進行強化，提升整體資訊韌性（Information Resilience）的能力，一定可以達到相輔相成之效。

但最重要的是，組織對於自身所訂定出來的制度或程序規範，一定要秉持「Fit for use」、「Fit for purpose」的原則，而不要為了資安而做資安。