資訊韌性如何助企業在未來的供應鏈中立穩根基？

Toni Allen[1] | UK Head of Client Propositions at BSI

無論稱之為網路安全、資訊韌性(information resilience)或是線上安全(online safety)，大家普遍同意妥善保護企業的數位資訊，是一個漸受矚目的議題，組織為確保長期繁榮發展也必須慎重面對。雖然資訊數位化大幅地提升企業的生產力，卻也使組織更容易遭受安全威脅，例如電腦舞弊或詐欺、間諜行為、惡意破壞與網路摧毀攻擊(cyber vandalism)等。

雲端運算的快速發展、人力資源外包與企業數據資料委外處理，都使問題加劇。誠如 BSI 曾對資訊主管所做的調查顯示，其中 91%承認組織曾經成為網路攻擊事件的受害者。約一半曾遭受駭客試圖入侵，或因惡意程式而蒙受損失(兩種狀況均遭遇過的佔 49%)。

今年(2016)的 5 月 16 日到 20 日是營運持續宣傳週(Business Continuity Awareness Week, BCAW)，這個由營運持續組織(Business Continuity Institute, BCI)所推動的年度活動目的是為了協助企業了解遵循最佳實務進行風險管理的價值。有意插足於未來供應鏈的組織，將必須展現其能屹立於新時代具挑戰性的環境之中。BSI 認為資訊韌性屬於我們稱「組織韌性」(organizational resilience)的一部分，既協助組織克服時間的考驗，同時維持獲利，而且更重要的是確保安全。在我們看來，無論是大企業還是小公司要具備組織韌性，三個最重要的領域就是建立資訊韌性、營運韌性和供應鏈韌性。

[1] 原文連結：http://www.infosecurity-magazine.com/blogs/information-resilience-secure/

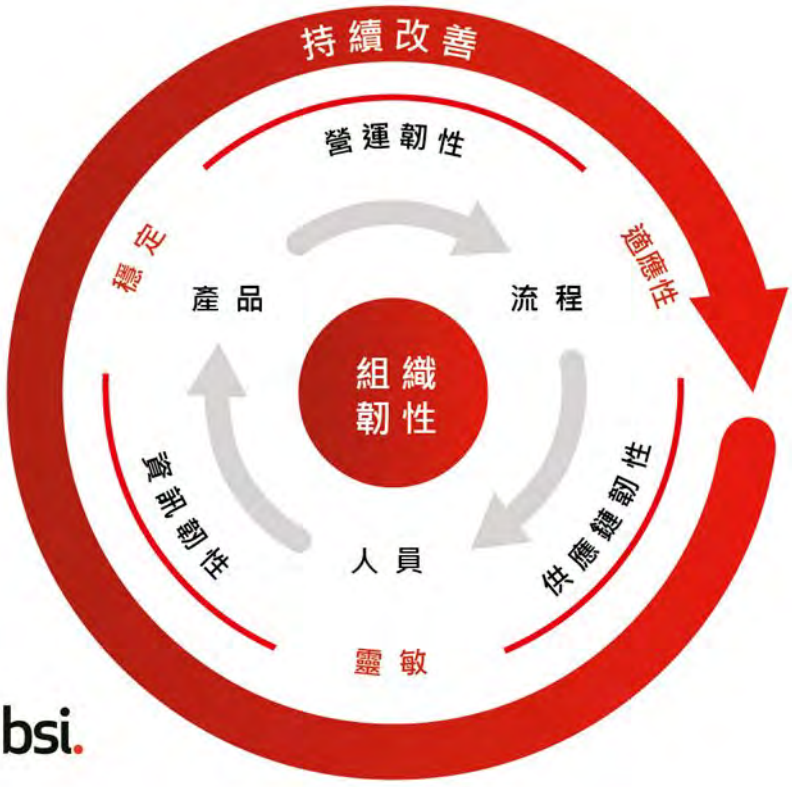
營運韌性
聚焦於組織營運提升，包含產品、服務與流程的績效和永續性。

資訊韌性
管理組織的實體、知識與數位資訊，從資訊的產生到銷毀，利害關係人都能安全有效率的儲存、取得及使用資訊。

供應鏈韌性
量化和緩和供應鏈風險的能力，包含採購、製造、運輸、銷售的生命週期，將供應鏈中斷的衝擊減至最小，以及保護組織免於財務和聲譽損害。

bsi.

很顯然地，資訊是組織內部進行績效管理、確保作業流程可信以及保障最終產品品質的重要因素。它是維持信賴與透明度的關鍵，不僅與客戶，也包含供應鏈關係。



某些威脅並非來自外部，而是因為內部的作業不當，例如誤用或未能運用情報，甚至是人為失誤或無做為。本研究也發現四成(42%)企業曾經歷可信賴的內部人員安裝未經授權的軟體，且將近三分之一(30%)遭遇過機密資訊的損失。

在當今的數位世界裡，個人與企業客戶都要能夠信賴與自己互動的公司，並透過充份的協議內容來保護自己的敏感資訊。同樣地，這些公司也必須確信採取的措施提供他們所需的保護。令人憂心的是，我們的研究顯示情況並非如此，雖然絕大多數的組織(98%)都會採用各種方法，以降低他們資訊安全面臨的風險，但對於組織抵禦外部攻擊的措施深具信心的僅有 12%。

在這些情況之下，標準可以提供幫助。安全架構的最佳實務包括 ISO/IEC 27001 資訊安全管理、政府支持的網路要素計畫(the Government-backed Cyber Essentials scheme) 以及 CSA STAR 認證或 ISO/IEC 27018 (專門針對雲端安全問題) ，均可協助組織受益於銷售增加、減少安全問題以及保護聲譽。此外，消費者辨識度高的標幟，例如 BSI 安全數位交易風箏標誌(Secure Digital Transactions Kitemark™)，便可讓已經實現這些標準的組織展現其實力。每個組織都有責任確知自身的弱點或風險為何，並且採取最佳方式提升自身的韌性與機會。

資訊長們難免會焦慮。幾乎每天都有新的網路威脅或資訊外洩情況，再加上必須隨時跟上此一領域中各種規範的潮流。這些威脅都是真實存在的，但是藉由仔細與誠實地審視數位供應鏈，並且將之視為更廣泛營運的一部分，有效地克服威脅並非不可能。如果能夠做到，則意味著組織將能夠運用經驗並且掌握機會，爲未來做好準備。

更多組織韌性的資訊，請造訪 BSI 集團 Organizational Resilience 專頁>

BSI 英國標準協會
+886 2 26560333
infotaiwan@bsigroup.com
www.bsigroup.tw