如何有效整合資訊安全與IT策略

各大組織看見了資訊安全深度嵌入其整體 IT 策略的未來，本文告訴您達成此目標之方法。

文／Bob Violino 譯／雲翻譯

資訊安全已成為IT不可或缺的一部分。在越來越多的公司行號中，從組織的角度看來，兩者幾乎已無法區分。

許多公司正在嘗試將資訊安全策略與IT策略本身更加緊密結合。這意味將採取部門整併、改變領導階層結構、在開發流程中提早嵌入安全措施，及其它相關策略。

根據CIO雜誌舉辦的2019年資訊長現況調查(State of the CIO survey)顯示，大約三分之二的企業組織認為其資訊安全策略和IT策略是緊密結合的，資訊安全是IT產品開發藍圖及專案計畫的關鍵元素。

但展望未來，兩者變得更加難以區分，83%的組織希望在未來三年內，將資訊安全策略緊密整合至整體IT策略中。

安全顧問公司 Moss Adams 的網路安全資深主管 Nathan Wenzler 提到：「我認為未來IT與安全策略會緊密結合，但結合的方式會與過去幾年看到的不同。」

Wenzler表示：「資訊安全通常僅被視為IT部門的一小部分，而且只是管理防火牆和垃圾郵件過濾器等安全工具的地方，但現在我看到越來越多資安團隊名實相符了——他們真正肩負起了風險管理功能。」

風險管理與如何減少風險就是IT與安全策略最緊密結合之處。舉個常見的例子：應用程式的安全性。Wenzler說，現在資安團隊更加關注如何將程式碼安全地從開發人員的測試平台持續轉移到生產環境，並在過程中進行適當的測試和控管。

安全策略能夠指出哪些領域可能因人為過失或錯誤，導致程式碼受損或失效，並建議應採取之措施以緩解或消除上述風險。

「IT團隊隨後介入，確定哪些工具最適合現有基礎設施，接著與現有開發工具和流程整合，並利用最適合的技術貫徹資安，」Wenzler說：「這是運用現代策略最理想之處，資安團隊也無需成為IT專家，反之亦然。」

以下列舉如何將資訊安全作為更緊密整合至IT策略中的方法。

一、授權高層安全主管

將IT與安全結合並不是將權力從安全管理人員手中奪走；事實上，他們應該在策略規畫過程中獲得更多發言權。

儲存、伺服器和網路硬體維護服務公司 Park Place Technologies 的資訊長 Michael Cantor 表示，IT策略和資訊安全策略已緊密整合，而網路安全領導力扮演了關鍵角色。

Cantor說：「我們的資訊安全主管出席了所有策略討論，包括年度預算週期。他策劃了一個為期五年的開發藍圖，其中包含了每個安全功能的目標，以確保在每一年中取得預期的進展。」

例如，其中一個目標是提高漏洞掃描的內部能力，以便 Park Place Technologies 能夠以更低的成本進行更頻繁的掃描。此目標已經特別納入基礎設施功能的2019

年度目標。Cantor表示，這個年度目標已被轉化為實施內部掃描技術，以及專注於使用該技術進行更頻繁掃描的專案。

資訊安全功能需要處於組織的適當層級，資安主管若不是直屬公司執行長，也至少須直屬資訊長。他認為：「為達成守護資訊安全的任務，獨立性是必要的，以確保資安資源不被其它IT職能（如：基礎設施）佔據。」

二、在整合方面獲得管理階層的支持

由於缺乏組織中最高階主管的支持，有多少計畫最終不了了之？IT與資安整合可能面臨同樣的命運。

「一定要獲得董事會、高級主管和領導團隊的支持，」全球家具設計和製造公司Haworth的隱私專員 Joe Cardamone 說，「網際網路上有大量關於及早整合資訊安全架構和策略的優點的相關資訊。」

Cardamone認為，向領導階層說明益處，使其接受並支持，有助於打破障礙。此外，若高階主管了解資安的價值，他們就更有可能看見IT與資安整合的價值。

「我們必須說明資訊安全如何促進業務發展，而不僅是工作流程中又一個麻煩的步驟。」Cardamone說。

當IT與資安各自能直通高階管理人時，情況會更好。

Rosendin Electric 公司是一家電氣承包商，該公司網路安全與法令遵循資深主任 James McGibney 表示，這樣的直通關係是不可或缺的。「幸運的是，我們的網路安全團隊在我們的IT組織內，直接向公司資訊長和執行長報告，資訊長、執行長，以及本公司所有高級主管都非常支持團隊正在進行的IT與資安工作。」

McGibney說，向高級主管直接報告的過程「完美無缺」，「公司高級主管完全理解保持強而有力的資訊安全力量有多麼重要。如果資訊團隊迫切需要導入安全解決方案，他們總是堅定支持我們。」

三、經常溝通並建立關係

在IT和資訊安全人員間建立良性溝通關係的需求不容小覷，對於有效整合至關重要。

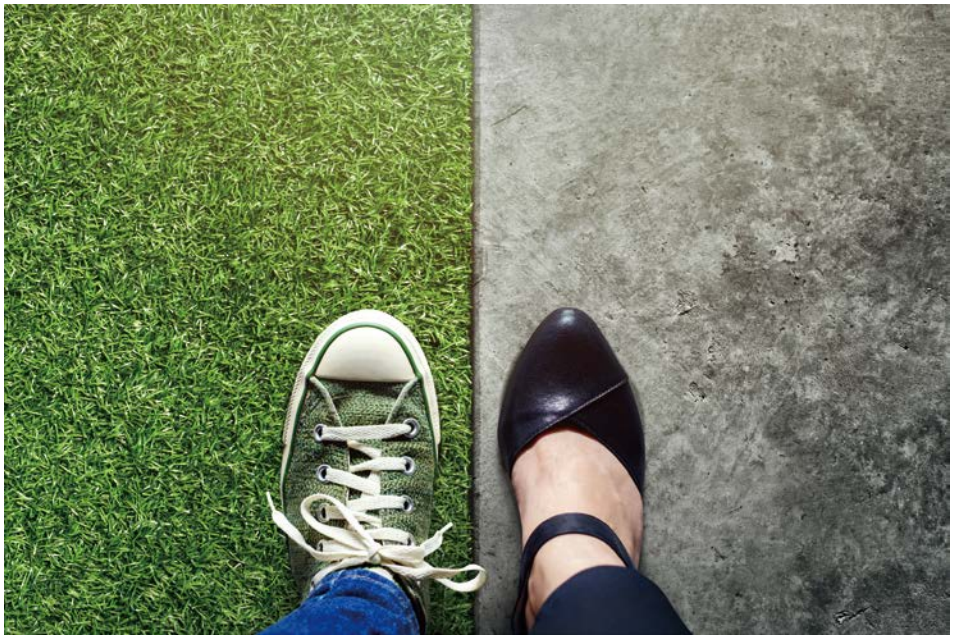
在 Rosendin Electric 公司，兩個領域之間的溝通極其關鍵。

「人的因素是目前任何IT組織面臨的最大風險，」McGibney說。「成功的網路釣魚活動很容易讓一間公司陷入癱瘓狀態。為了建立真正的防禦縱深，IT和資訊安全團隊需要共同努力，在攻擊面上實施解決方案，無論解該決方案是在辦公室內或雲端執行的。資訊安全團隊實施的政策足以影響基礎架構，而基礎架構端實施的政策也足以影響資訊安全。雙方真的得攜手並進。」

Wenzler認為，IT和資安團隊必須了解他們想達成什麼目標，以及為什麼這個目標對組織很重要。他強調：「當雙方互不溝通時，很容易造成風險策略與技術目標不一致，雖然職責不同，但他們是彼此成功的必要條件，因此如果沒有持續溝通，便會造成步調不一。」

這兩個領域間一定要建立更加良好的關係。Cardamone說，資訊安全人員有時被視為專案進行的障礙，妨礙工作流程。

為了促進溝通管道暢通，資訊



安全團隊需要強調合群的精神。

Cardamone表示，在Haworth，IT工程師和資訊安全團隊每月舉行會議，討論即將發生的變革、專案、挑戰以及對任何一方都有益的其他問題。他說：「這類會議能產生效果的原因是領導團隊支持這樣的行動，且不鼓勵IT人員中常見的獨立作業行為。」

將資訊安全作為更緊密整合至 IT 策略中的方法

一、授權高層安全主管。
二、在整合方面獲得管理階層的支持。
三、經常溝通並建立關係。
四、善用安全標準並使用可比較的指標。
五、為公司的產品建構資料保護機制。

四、善用安全標準並使用可比較的指標

希望整合IT和資安的公司應考慮使用標準安全架構，例如由美國國家標準暨技術研究院(NIST)建立的安全架構，以設定資訊安全環境的目標。

Cantor說：「安全架構設立後，便能建立資訊安全藍圖，可以有效地排定優先事項，並與所有功能共享，以訂定年度目標。」

使用架構來標準化公司內部的安全操作，可確保資訊安全的所有面向，並可針對風險和成熟度目標確定優先事項。只要一間公司選定一個架構，並根據該架構對特定情況的適用程度來部署各種元素，「那家公司基本上就建立了安全策略，」Cantor說，

「資訊安全能夠在其自身的功能中實現特定的目標是非常罕見的。通常它需要結合其他功能來實現資安目標，因此與整體IT策略能否完成整合是成功的關鍵。」

除了標準之外，IT和資安團隊還應該使用可比較的指標，以免混淆終極目標。

Wenzler說，很多時候資安團隊開始以無關IT團隊或營運職能的方式衡量風險甚至成功與否。

「同樣的，正常運作時間的量測或服務台的回應可能觸及『完整性和可用性』這兩大資安支柱，但無法適當解決風險問題，確保每個人都了解所使用的指標，並善用可因技術改進而揭示風險降低的指標。」

五、為公司的產品建構資料保護機制

有效的IT和資安整合應擴展到公司為其客戶提供的產品和服務，並在內部使用——各行各業皆然。

「在我們的IT產品中建構資料保護至關重要。」McGibney說。例如：將公司手機分配給員工時，會立即在統一的端點管理系統中完成註冊。如果員工攜帶自己的電子裝置處理公事，也必須進行註冊，否則不得以該裝置存取任何公司資源。

McGibney說：「隨著網路釣魚活動漸趨猖獗，任何公司都冒著員工點擊冒牌網站、然後輸入登入憑證的風險——一旦成真，結局大家都清楚。駭客不僅可以無限制地造訪您的 Active Directory 基礎架構，他們還可以存取您的流程和程序。而這通常會導致火力更集中的網路釣魚攻擊。」

物聯網(IoT)擴大了攻擊面。McGibney表示：「任何接觸過網際網路的一切都能成為公司的潛在進入點，手機、平板電腦、筆記型電腦、桌上型電腦、安全攝影機、照明控制器、恆溫器、虛擬實境(VR)設備等，以上所有設備都需要實行某種修補管理和弱點管理流程。」

McGibney說，駭客堪稱世界上最聰明的一群人。「當駭客確定並專注於滲透你的環境時，他們將使用任何必要的手段來達成目標，無論是透過社交工程或是網絡釣魚活動，因此企業必須隨時保持警惕和提倡安全意識。」