[**雲端運算安全的五大迷思**](http://domynews.blog.ithome.com.tw/post/1252/74657)

**蔡明朗譯**

原文來源：Top 5 Myths of Cloud Computing Security

IT 產業分析以及媒體報導時，發現到許多矛盾的觀點。某些作者認為雲端運算較為安全，有些則特別強調新的安全挑戰。由於雲端的概念目前仍在雛形階段，因此到處充斥著許多似是而非的論點。以下是最常聽到的五大雲端運算迷思：您能輕易和 VMware 合作進行現有基礎架構投資的虛擬化，包括伺服器、儲存設備和網路，以建立電腦運算資源的高可用性集區。將服務層級政策套用至應用程式，VMware 可以讓使用者更能控制佈建及支付 IT 服務。再加上，VMware 只提供共通雲端運算基礎架構平台，連結私有與公用雲端資源，建立混合式雲端架構。立即開始使用 VMware 建立私有雲端。

**雲端運算基礎架構**



**迷思1)  基礎架構服務 (Infrastructure-as-a-Service，簡稱 IaaS) 供應商所提供的虛擬私人雲端就像企業內部資料中心一樣安全。**

「虛擬私人雲端」是 IaaS 領域所衍生出來的新興概念，可讓企業透過虛擬私人網路 (VPN) 連線至雲端的資源，IaaS 廠商會提供一段企業專屬的 IP 範圍。這種運算方式的問題在於您仍舊與其他企業共用硬體資源與交換網路，彼此間僅藉由虛擬區域網路 (VLAN) 隔離。然而組態設定錯誤的情況時有所聞。根據最近一份[研究](http://www.securecomputing.net.au/News/171606,data-breaches-to-cost-more-in-the-cloud.aspx)顯示，澳洲有 31% 的資料外洩事件是「第三方廠商如雲端運算或 SaaS 供應商的錯誤所造成」。

**迷思2)** **您不需要一家以上的 IaaS 供應商。**

將所有雞蛋都放在同一個籃子，萬一籃子打翻了就很危險，雲端運算也一樣。雖然採用單一 IaaS 供應商較容易管理，但卻也形成單一故障點。仰賴單一IaaS供應商的風險是，萬一廠商遭到分散式阻斷服務 (Distributed Denial of Service，簡稱 DDOS) 攻擊，企業的營運就可能發生中斷 。另一個單一故障點 (SPOF) 的例子是Rac space，一輛卡車撞上了某個變電箱而導致 Rack space資料中心電力中斷，業務因而停擺。由於意外在所難免，因此，要防止單一故障點，就要擁有一家以上的 IaaS 供應商。

建立備援據點，是達成災難復原的主要方法之一，雲端運算的時代也一樣。企業或許不需要一個熱待命的失敗接管據點，但卻應該規劃並測試如何在需要的時候迅速將營運切換至第二家供應商。雖然像 Amazon「可用性區間」這類的作法可降低上述風險，但並不能完全消除單一故障點的可能性 。

**迷思3)** **私人雲端同樣也適用實體資料中心的安全方案。**

其思維邏輯是，資料中心原本的邊境防禦就已成效良好，而私人雲端也受到同樣的保護，所以應該沒問題。只可惜，情況通常並非如此。私人雲端 (或稱為動態虛擬化資料中心) 有其新的挑戰，這些挑戰是傳統靜態資料中心所沒有的。虛擬化與雲端運算加大了歹徒的攻擊面，共用式儲存就是一個例子。

另外還有一些新的狀況，例如系統管理員不小心用某個伺服器從安全區域移到 DMZ。此外組態設定錯誤也可能導致資料未妥善隔離。還有，同一個 shield 區域內的 VM 之間不受監控的資料流量呢？在一個混合式雲端環境中，當一個應用程式移到雲端，其虛擬機器周圍卻沒有安全防護將會如何？仰賴 IaaS 廠商所提供的基本防火牆規則，甚至連 IDS/IPS 也沒有，可能會讓某些企業感到不安。

**迷思4) 雲端服務供應商會負起安全的責任**。

雖然SaaS或 PaaS服務供應商通常會在服務條款中提供安全保障，在IaaS領域卻不然。雖然IaaS廠商會採取一些安全措施，並且在文宣中強調其安全措施，但IaaS環境的安全性終究是企業與IaaS廠商應該共同負擔的責任，而且，最終的責任通常還是落在企業本身。您IaaS 供應商的服務條款中有關安全的章節應該會強調這一點。

不僅如此，雖然供應商會負起安全的責任，但萬一發生資料外洩事件，企業本身仍舊須承擔最終的責任。畢竟，那是您的資料。

**迷思5) 我的雲端服務廠商**

稽核的確是不錯的安全基礎，也是確保廠商在檢查期間安全控管措施正常運作的一項工具，但這並不等於安全性。而且可能給人一種安全感的假象。稽核所看的是過去的狀況，雖然過去的績效對未來具指標性 (至少在資料中心安全方面)，但絕非未來的保證。一旦公司發生大規模或不預期的人事變動，就可能讓原本紮實完整的安全措施一夕之間瓦解。也無法防止心生不滿的員工對公司或客戶挾怨報復。

稽核無法檢查稽核範圍以外的項目。在稽核檢查表上的項目您或許嚴格控管，但漏洞卻可能在檢查範圍之外。再者，任何流程的稽核都無法涵蓋執行流程的人。廠商的用人原則為何稽核並不一定涵蓋用人原則。凡人都可能犯錯，當然也絕非完美 (純粹就事論事)。

審查並沒有一套標準作法。這類稽核是稽核者與受稽核對象彼此共同設計出來，目的在於測試特定業務流程的控管措施。而控管措施可能無法「包山包海」，所以，在原先預定之外的項目，即使對業務服務很重要也不在測試範圍內。因此，在將關鍵業務流程交給任何服務供應商之前，您應該對稽核有所存疑。而且，理想的稽核不應該只專注於資料安全，而是應該延伸至服務永續性、廠商管理、備份復原、人事制度等其他領域。

不論公共雲端或私人雲端在降低成本、提升企業靈活度方面都能提供優異的企業價值。不過，建議您在挑選之前還是應該先認清其中的安全挑戰。