Grant Thornton An instinct for growth™ 正大專欄

雲端網路安全風險管理

賈泉德

近年來發展雲端技術及互連網是各大產業的趨勢，雲端技術將檔案資源及商業活動轉移到虛擬平臺上，而不是特定在某一處所，業者可以因而更靈活、快速、廣泛、透明、安全、便宜的提升資料管理方式。

為了因應最近推出的歐盟個人資料保護法（GDPR）等新資料保護規定，許多業者都需要提升更高的資訊安全防護。**對於每間公司來說，採用新的雲端技術服務，也可能帶來新的風險，還是要保持謹慎。**

在現今的網路環境中，沒有什麼可以保證百分百安全的，我們應該意識到雲端技術可能帶來的一切風險利弊，多花一些時間來識別這些雲端供應商，是否有真有制定可靠的資安防護策略，所以關鍵就是要盡最大可能降低這些風險，才能**更安全的體驗雲端服務，我們可以從以下二點開始著手：**

一、評估我們的需求

在找到合適的雲端供應商之前，我們需要確定哪些資料需要上傳到雲端，哪些資料要保留在我們自己的機房中。進行這樣的分類時，我們需要先制定檔案相關性、敏感性以及保護檔案所需的政策，從這裡我們可以決定將哪些資料保留在公司內，或要儲存在雲端，還是完全刪除。例如，我們可能會選擇將敏感的資料儲存在公司內（如研發或專利資料）；再來，我們需要選擇最適合的安全措施，實體安全（如室內環境、刷卡門禁、攝影機等）、公司內部保密流程（如員工資安教育訓練、公司營運計畫等）、銷毀不需要的資料、以及採用技術措施（如加密技術、防火牆等）。

二、雲端供應商水準參差不齊

許多公司採用雲端儲存資料，是因為對於資料存放的地點及備份方面來說，比傳統的網路儲存更安全，但使用雲端服務並不能完全保證我們的資料絕對不會外洩或被竊取。與大多數的商品一樣，費用最低的供應商通常會帶來較大的風險，我們務必要提早進行規劃，確認我們所需要的安全等級，並找到可以提供這些充足防護的供應商。即使選擇了高端供應商，也無法絕對保證我們資料的安全，這一點的認知很重要。

在確認我們所需的服務後，**要確認的是供應商的義務和責任範圍，例如技術安全措施、規則的透明度、法律責任等，**並同時瞭解我們自己的義務，提早提出正確的問題並弄清所有不明的細節，同樣也是重要的。如果對方可以在我們的預算內，且可以針對我們擔憂的弱點來填補資料安全漏洞，那麼我們可能已經找到了合適的供應商。

最後，當我們每次使用這些新型態的網路服務時，都是給駭客創造新的攻擊目標；同樣的，**我們在使用這些新服務前，也都必須先識別新的風險，並確保我們具有適當的額外保護措施，**為了能在新科技時代中保持競爭力，公司需要不斷擁有新技術，但也務必自我謹慎及選擇，以獲得最佳結果。

（本文作者Grant Thornton Taiwan正大聯合會計師事務所經理）