

沒有一個資訊系統是絕對安全的，
所以不要把重要資料放在自己無法控制的地方。

你用的雲安全嗎？

◎魯明德

雲端是近年的顯學，企業沒有用雲端、個人不知道雲端，好像就落伍了；很多企業為了顯示自己跟得上時代的潮流，不但號稱資料放在雲端，甚至連資訊系統都在雲端運作。

就在雲端概念風起雲湧之際，據報載某水果牌手機推出的雲端服務 iCloud 遭到駭客入侵，大量好萊塢女明星儲存在 iCloud 的私密照被盜，甚至一些已經刪除的照片都被駭客盜取，並在網路上流傳。

看到這則新聞，在科技公司任職的小潘，馬上想到自己公司所用的企業資源規劃 (Enterprise Resource Planning, ERP) 系統，也是一個放在雲端上的系統，這樣做到底安不安全呢？在這個月的師生下午茶約會中，小潘決定把雲端的安全問題拿出來跟司馬特老師討論。

在充滿焦糖瑪琪朵咖啡香的週末下午，小潘一見到司馬特老師，就迫不及待地提出他的疑問：水果公司當初在建置 iCloud 系統時，難道沒有考慮到資訊安全的問題嗎？

司馬特老師喝口咖啡娓娓道來，不要認為有了防火牆就可以解決所有問題，我們應該認知：沒有一個資訊系統是絕對安全的，所以要養成一個習慣，不要把重要的資料放在自己無法控制的地方。

iCloud 的安全機制怎麼運作？到底有多安全？我們都不知道，甚至於像這次的事件是怎麼發生的？系統的漏洞在哪裏？我們也不知道，相信他們也不會告訴我們。所有的使用者都只能從他們的官網上獲得安全相關訊息。

從官方網站公布的資料來看，使用者上傳過程跟儲存在 iCloud 的文件，都是以 128bit 的金鑰用 AES 方式加密；官方的 APP 也有身分驗證機制，會確認用戶的帳號和密碼，而發送給第三方服務的訊息也是用 SSL 處理。至於使用者所用的帳號密碼，系統也要求要包含數字、大小寫字

母，且至少要 8 位字元。至於在系統的使用上也有雙重認證的機制，以降低用戶因帳號資訊被盜而遺失資料的風險。當用戶首次使用手機和平板電腦登入 iCloud 時，系統會發出一個 4 位數的驗證碼至用戶的手機，驗證成功後授權該裝置可以登入用戶的帳戶，並在其他曾使用該帳戶的裝置彈出通知，告知用戶該帳號在何時何地登錄 iCloud。

小潘聽到這裏，直覺的反應是：既然 iCloud 有這麼完善的安全機制，為什麼又會造成照片外洩呢？司馬特老師喝口咖啡後笑著說，系統的漏洞很多時候是人為因素造成的。以這次事件來說，危安的系统因素還不明朗，但雲端資料的安全議題可分為幾類：第一類是個人密碼的問題，使用者設定的密碼若安全性不夠，就容易遭到駭客的暴力破解；其次，很多人為了方便，所有系統都用同一個密碼，只要一個密碼被破解，就全部淪陷了，所以比較重要的密碼，還是要另外設定，不要跟 e-mail 信箱用同一個。第二類則是系統資訊安全的問題，iOS 一向給人的感覺就是資安問題沒有 Windows 這麼多，所以很多 iOS 使用者的戒心就降低很多。一般資訊系統雖然都裝了防毒軟體，然而資訊安全不可能做到百分之百的安全，偶而還是防不勝防，像木馬程式可能會把存在電腦中的帳號密碼，在你不知不覺中傳了出去；還有一些釣魚程式會偽裝在郵件中，使用者不知情地打開，帳號密碼就有可能被竊走。

小潘聽到這裡，想著如果不用雲端運算，是不是就比較安全呢？司馬特老師似乎看出小潘的心思，接著表示：我們生活在科技時代是不能當駝鳥的，以為把頭埋在土裡就安全了，事實上資訊科技是用來幫助企業做管理，給我們更方便的生活，我們不必因噎廢食，畢竟任何事情都有風險，端賴我們事前縝密的風險管理；在追求效率與便利的需求下，雲端運算應是一條無可避免的不歸路，然而，面對不斷推陳出新的危安事件，我們應該要有風險意識，要隨時檢討各種危安因子，並採取有效的阻攔措施，以降低其發生的機率；而這些措施不能是一成不變的，當敵人越來越厲害的時候，我們的防禦工事也要相對地與日俱進，才能有效防止危安事件的發生。

(作者為科技大學資訊管理系講師)