雲端下員工個人行動裝置的管理

◎魯明德

由於網路的普及與行動裝置的功能日益強大，加上雲端運算的推波助瀾，使得企業在資訊基礎建設上，出現兩極化的發展；在 X86 虛擬化技術逐步成熟下，處於後端的機房管理，集中化的趨勢越來越明顯，機房的伺服器是整併再整併，系統也是不斷集中，甚至連原本分散在世界各地工廠的機房，也有收回總部統一管理的趨勢。

但是，前端的客戶端，卻是朝向完全相反的方向發展。由於近年來智慧型手機、平板電腦的風行，前端使用者的裝置類型變得多樣化。未來，讓員工使用私人設備來處理公事，已經被許多大企業採納，即使像美國國防部這樣的機敏單位，都已同意員工使用自己的裝備上班。未來前端的發展趨勢將會日益分散，不再像過去只是 PC 單一平台。

小潘所處的高科技公司也趕上這個潮流，以往公司為了讓工程師 24 小時待命，都會配發一支手機給工程師；小潘就常常自嘲是雙槍俠，左右各配戴一支手機。隨著時代的進步，自己的手機已換成智慧型手機，而公司配發的仍然是傻瓜型手機。這個月開始，公司索性收回公發的傻瓜型手機，開放所有員工使用自己的智慧型手機、平板電腦或筆記型電腦等行動裝置，透過公司建置的無線網路環境，直接存取公司內部網路的資訊。

對於公司的這項政策，小潘有點適應不良，心想：這樣不就門戶大開，歡迎大家來偷機密資料了嗎？趁著這個月的師生下午茶約會，把他的疑慮提出來。司馬特老師喝口咖啡後娓娓道來。

目前國外有一些大型企業，包括 IBM、HP 等跨國公司，都開始開放員工使用自己的行動裝置，在確保資訊安全的前提下，讓員工上班時使用自己喜歡的智慧型手機或平板電腦，以提升工作效率，這樣的風潮稱之為「員工自帶設備」(Bring Your Own Device，簡稱 BYOD)。

根據英國調查機構 Vanson Bourn 在 2011 年的研究顯示：開放員工帶自己的行動設備上班，有 78%的上班族認為，員工自己帶的電腦一定比公司提供的電腦效能更好。最重要的是，企業若推動 BYOD 的策略，員工會認為公司的管理思維比較先進，可以提高員工對企業的認同感，員工對於工作的滿意度也比較高。

國內的永慶房屋直營或加盟店的房仲經紀人，都是使用自己的 iPad，配合公司「i 智慧經紀人」的系統，提供看屋客戶最即時的服務，因為 iPad 是員工自己掏腰包購買的，也會相對珍惜使用。

小潘聽完司馬特老師的解釋，仍然惦記著資訊安全的問題，看老師都沒有提到，於是繼續追問下去。司馬特老師喝口咖啡接著說：員工自帶設備來上班，對公司的資訊安全確實是一大考驗；但是，如果能做好安全控管，將會是創造員工與公司雙贏的局面。

在員工個人自帶設備的安全控管上，首先要做的是身分認證與存取管理，要求員工的自帶設備上必須安裝公司提供的代理程式或 APP 程式，在登入時可以做身分認證之用，存取資料時，亦可做權限管理之用。其次，要建立行動裝置管理（Mobile Device Management，簡稱 MDM）機制，藉由螢幕的鎖定、遠端鎖定等操作，保護資料不被竊取，甚至在裝置遺失時，可以透過遠端刪除的功能，將公司資料刪除，以防機密資料外洩。

最後，透過虛擬桌面架構（Virtual Desktop Infrastructure，簡稱 VDI），員工日常工作所需的應用程式、資料庫，都是由後端的伺服器提供，操作過程中所產生的資料，也不會留在員工的自帶設備上，統統儲存在後端的伺服器裡；所以，客戶端的行動裝置就像是一個終端機，可以解決機密資料外洩的問題。

小潘聽完司馬特老師的一番解說，也有了另一層心得：原來資訊安全不是一味地防堵即可萬無一失，適當地採取資訊科技與管理措施，也可以化危機為轉機。員工自帶設備上班的現象，對企業來說就像是雙面刃，可以為公司節省採購硬體的成本，也能提升整體工作產能，但也有造成危安的風險。

行動裝置本身不是問題，資訊科技所要關注的，應該是行動裝置取用企業資料過程的安全管理，尤其是裝置的身分識別、網路存取等級和行動應用系統的管理措施，越早部署、效果越好。