行動裝置的安全管理

◎魯明德

在資通訊環境日益進步之際，除可看到很多人邊走邊滑手機外，我們在餐廳、捷運、車站各處，也都能看到人們滑著手機，專注於自己的社群網站、即時通訊軟體，或在處理公司的事情；不管是哪一種，這些行為都顯示我們在日常生活中對行動裝置的依賴越來越深。

根據研究機構 Gartner 調查指出，全球至 2016 年將有 38%的企業停止配發資通訊裝備給員工，而讓員工直接使用自己的資通訊裝備來公司工作；趨勢科技也進行類似的調查，70%的受訪企業認為讓員工使用自己的裝備來公司工作，能強化工作效能、降低企業成本，不過也有 85%的企業擔心因此會提高企業資料外洩的風險。

就在今（103）年 7 月底，蘋果首度鬆口承認 iOS 有後門程式，使用者在 iPhone 上的簡訊、通訊錄、照片等個資，都有可能經由這個後門被竊取；至於 Android 系統有沒有這個漏洞，尚不得而知。7 月初，行政院消費者保護處也公布一項委由資策會資安科技研究所進行的抽樣檢測結果，發現三大智慧型手機品牌的資訊安全系統都存在著資訊安全疑慮，這些資安疑慮可歸納為兩大類：重要資訊未加密就

儲存、連結不安全的網站時手機不會主動告知。因此，使用者的私密資料可能輕易被駭客竊取，成為網路犯罪的受害者。

看到這些企業發展趨勢與系統安全的報導，從事高科技工作的小潘開始擔心：目前員工上班所用的電腦是由公司統一配發，可以在電腦上做些資訊安全的防護措施，未來如果讓員工自備電腦變成一種主流，資訊安全要怎麼管制呢？現在連封閉系統的 iOS 都有資安的疑慮，那麼號稱是開放式系統的 Android 會不會也有不為人知的漏洞呢？在這種複雜的環境下，企業的資訊安全如何維護？

帶著這麼多的疑問，小潘在這個月的師生下午茶約會中，把這些問題逐一提出跟司馬特老師請益。司馬特老師喝口咖啡後，先對小潘分析當前的產業趨勢，由於 3G 與 Internet 技術的成熟，加上行動裝置普及，造就了企業將電子化延伸為行動化的趨勢。

以往房屋仲介業者都要準備很多的紙本、照片等資料，才能跟客戶推薦物件，而且只能在店裡才有資料可看；現在，各個房仲公司都開發出他們自己的系統，讓仲介業務員透過手機或平板電腦就能提供購屋者各種參考物件，甚至可讓賣屋者自己上網去張貼物件資料。考量人員的流動及裝備的購置成本，未來仲介人員的手機、行動裝置都可能會讓他們自己去購置。當裝備是自己的，很容易就會公私混淆，

裝備裡面有公司的資料，也有個人的資料，這時，資訊安全就很重要了，如何能讓公司的資料不外洩，就成了資訊部門的一項重大挑戰。

這可從三個方向來思考，首先是員工認證，必須是合法的員工才能透過裝置登入公司的系統，為了簡化員工的作業，可以將認證及安控機制寫成一個 APP，所有員工自己的裝備都要安裝這個 APP，才能登入公司的系統，如此可以防止非法登入。經由認證賦予使用者包括存、取、讀、寫等必要的權限，以避免使用者看到不該看的機密資訊。其次是資料的處理，在系統設計時，應盡量把工作放在 server 端來執行，以減少 client 端的資料存量，讓資訊集中存放，即可減少機密資訊在 client 端被入侵竊取的風險。

為避免合法的使用者對機密資料的監守自盜，除了在管理面上從規章制度去要求外，也應透過系統設計加以防範。這點可以結合前述之認證與權限管理，當資料集中管理後，就要嚴格控管員工下載資料的權限，可利用系統讓員工不能輕易地下載資料；即使有權限下載資料的員工，系統也要對下載的內容做成紀錄，以便日後追蹤；對於異常的下載，則要隨時出現警訊，讓系統管理者可以立即採取危機處理措施。

小潘聽到這裏，對資訊系統的安全管理有了更深一層的了解；但是，他又想到另一個問題，上個月他遺失了一支手機，將心比心，員工的手機也可能會遺失，撿到手機的人，不就可以堂而皇之地進入系統，看盡公司所有資料嗎？

對於小潘的舉一反三，司馬特老師很高興地表示，這也是管理層面的問題，我們的信用卡遺失，可以打電話到銀行掛失止付；同樣地，公司內部也必須建立一套機制，當員工的裝置遺失，要提供一個窗口讓他能掛失，這時，該裝置上的認證碼就會被終止，撿到手機的人就無法登入系統，而此一掛失的窗口可以是人，也可以透過系統來掛失。

小潘聽完司馬特老師的一席說明，深感企業讓員工用自己的資通訊裝備上班，是未來的趨勢，不但企業可以減少成本，員工也會因為用自己的裝備比較順手而提高工作效率；與其以資安問題跟員工對抗，不如提早針對資安問題，提出解決方案，從管理面與技術面雙管齊下，才可能創造企業與員工的雙贏！