客戶資料的安全防護

◎魯明德

據國外網路報導，多家銀行透過黑市購得一批金融卡資訊，而相關資料是從 Home Depot 外流而來，Home Depot 也正式承認該公司的多個支付資料系統被入侵，可能影響其在美國與加拿大商店使用金融卡消費的顧客。無獨有偶地，國內的中國信託網站繳費中心也爆發用戶的個人資料外洩事件，金管會調查後確定其內部程式設計、驗證，及內控程序上有缺失，導致大量用戶資料外洩，因而裁罰新臺幣 400 萬元。

從事資訊工作的小潘看到這些新聞，回顧自己的工作，由於公司跨入電子商務領域，資訊系統與網際網路的關係也日漸密切，自然也開始擔心客戶資料庫的安全問題，思考著萬一有資料外洩的事件發生，可能會造成無法收拾的局面。針對這些擔心的問題，小潘決定要利用這個月的師生下午茶約會，好好地跟司馬特老師討論解決方案。

司馬特老師聽完小潘的問題，喝口咖啡後娓娓道來，長久以來，大家習慣把資訊安全問題的焦點放在外部駭客的入侵，將所有的心力、人力、預算與防護重點，都放在外部威脅的防護上。但是，越來越多的實際案例與研究報告顯示，內部有心人士或管理疏失已成為企業資

料外洩的最大威脅來源，對於企業內部擁有合法存取權限的有心員工，毫無警覺與防備之心，已成為企業資料外洩最頻繁也最嚴重的主要原因。

早在 2005 年時，Vontu 與 Ponemon Institute 就已經共同發表研究報告指出，資訊安全的最大威脅並非駭客或病毒，而是惡意或粗心的企業內部員工。後來 Ponemon Institute 又在 2011 及 2012 年另外與 Symantec 共同發表全美資料外洩成本研究報告，指出玩忽職守的員工是資料外洩的最大元兇，絕大部分的資料外洩是由人為錯誤與系統缺陷所致。Verizon 所做的 2014 年資料外洩調查報告中指出，大約 58%的公部門網路安全事件肇因於內部員工，其中約 34%是員工在資料控管上的意外事故所造成，另 24%則因未經授權與惡意的資料濫用所致。

小潘聽完司馬特老師的說明後，認同地表示：怠忽職守或粗心員工造成的資料外洩還好補救，只要透過一定的加密機制，多少可以降低風險；最令人擔心的，莫過於擁有合法權限員工的有意之舉，甚至是擁有最高權限的主管或資料庫管理員，這些人可能造成不可挽回的損害。

司馬特老師非常認同小潘的看法，喝完咖啡也繼續說明，在實務上今（103）年也發生過案例，1 月下旬，可口可樂公司爆發 7.4 萬筆個人資料外洩事件，這些個資多半是社會安全碼與駕照號碼等敏感性資料，除了 1.8 萬名現職員工受到衝擊之外，大部分受到牽累的皆屬前任員工，而另外也有 4,500 筆個資是與外部承包商或供應商之員工有關。根據調查了解，該事件起因於前 MIS 人員將數十臺筆電偷走所致，由於被偷的筆電原屬人力資源部門人員所有，再加上筆電所有資料都沒有依照公司之安全政策進行加密，於是筆電裡的個人資料就這樣流落出去。

而 AT&T 早在 2010 年便曾發生客戶資料外洩的事件，因內部授權員工濫用存取行為，導致 11.4 萬筆旗下 Apple iPad 3G 綁約用戶之郵件地址外洩；今年又發生 3 名具備手機記錄存取權限的 AT&T 外部供應商員工，濫用存取權限竊取顧客生日及社會安全碼等資料，目的竟然是為了將 AT&T 綁約的手機解鎖，以便拿到二手市場上轉賣獲利。

小潘也認為具有權限的員工如果有心想要竊取存於系統上的客戶資料，一定是持續地五鬼搬運、不露痕跡，真是防不勝防，等到事發可能已經來不及了，應該要怎麼事先防範呢？

司馬特老師喝完咖啡繼續說下去，一般企業對員工的資安管理都很嚴格，但是對高階主管及具有系統管理權限的人，管理上往往相對鬆散；然而，容易洩密的卻都是這一群人。對於具有系統存取權限的員工，資料加密也是擋不住有心人士的竊取，這必須由管理面著手，首先要把公司的資料做機密等級的區分，密級以上的資料除應限制存取權限外，存放在系統或資料庫中時，還要另做加密處理。

而客戶資料是《個人資料保護法》保護的標的，又要特別小心處理，萬一不小心洩漏出去，每位受害人都可求償，最少賠償額度是500 元，積少成多甚至可讓公司倒閉。所以，對於公司的客戶資料，尤其是電子商務的廠商，客戶資料尤其多，僅是資料加密可能無法阻止具有存取權限的有心人士竊取。為了防止資料外洩，除了在制度上要加以限制外，系統設計時也要置入預防措施，因為有心人士所要竊取的客戶資料一定要數量很大，才有相對利益，所以，要利用系統設置監控機制，對於異常的資料下載，需要即時對其主管警示，以採取必要的防止手段。

經過這次的討論，小潘對於資訊安全又有了深一層的認識。資訊安全要防範的除了外部威脅外，其實內部合法人員的非法存取才是最可怕的，尤其是客戶資料又涉及個人資料保護，處置不當將對公司造

成無法彌補的損失，唯有透過制度跟系統雙管齊下，才能有效確保資訊安全。