制度建立分層避險｜保護個資不能只重視資安技術

王德瀛／財團法人資訊工業策進會科技法律研究所專案經理

論者表示，高風險的行業，可以考慮引入適當的個人資料保護與管理制度，透過制度建立的風險評估方法及不同層面的個資保護設計。示意圖，個資經馬賽克處理。資料照片

近日傳出疑似人力銀行個資外洩遭人放到暗網販賣，不久前也有醫療院所疑似遭到駭客企圖入侵竊取個資的案件。除了我國外，國際上英國航空、萬豪酒店等大規模個資外洩事件也令人記憶猶新。

事實上，人力銀行、醫療院所、運輸旅宿等組織，不是掌握當事人完整的生命歷程（學經歷、人格特質、醫療紀錄等），就是擁有當事人聯絡、付款等具有高度利用價值的資料。這些都是犯罪集團集中鎖定的目標。因此如何透過建立適當的個資管理制度來控制及降低個資事故的風險，減少商譽損失及可能的法律風險，是企業必須面對的重要課題。

每當遇到這類個資事故的新聞時，我們時常可以看到組織的高層承諾將採用更多的資安防護措施，或是在技術與硬體上進行更鉅額的投資。這些做法無非是希望透過在硬體及技術層面的投入，展現個資保護的決心，希望能重新獲得消費者的信任。

然而，個人資料的管理與保護，並不是在技術層面或物理層面上投入資源就可以畢其功於一役；如果沒有同時注意作業面的流程規劃以及在組織層面的人員訓練與管理，仍然會使個人資料無法獲得妥善的照顧。

舉例來說，多年前傳出的台北市愛滋病感染者個資外洩事件，就不是因為硬體或技術上的缺失，而是人員對於資料的重視程度不足，無意間將資料放置在其他單位的電腦，又忘記刪除才導致的。

類似的事情也不只是發生在台灣，去年10月，德國巴登-符騰堡邦個資主管機關宣布處罰一家醫院8萬歐元的裁罰，原因正式因為該家醫院製作數位出版品的時候，疏於檢查內容，導致患者的資料意外暴露在數位出版品之中。類似的狀況也發生去年7月的一起羅馬尼亞個資主管機關針對飯店裁罰案件，該飯店因為沒有注意到數位出版品中使用的照片還有紙本個資文件，導致文件內的個資意外的暴露，而被處以1.5萬歐元的處罰。

除了人員對個資的意識外，個人資料的流程設計也是降低個人資料風險的重要手段。去年6月，荷蘭個資主管機關宣布對一家醫院處以高達46萬歐元的處罰，而且如果未能即時改善每2周將再追加1萬歐元。之所以罰鍰的金額這麼的高，其實是因為該醫院沒有妥善的設計資料流程，導致病患的病歷會被許多醫院的職員多次、不必要的查閱，突然增加病患病歷發生外洩、遺失、損毀等的風險。流程的設計不良不只是潛在的法律風險，甚至可能引發其他的紛爭。

去年12月德國萊茵蘭-普法茲邦的一家醫院因為未妥善設計患者入院資料的分類、歸檔等流程，因為資料的混亂造成住院費用計算錯誤，除了被主管機關處罰10.5萬歐元的罰款外，也因為這些費用計算的錯誤而衍生後續與患者間的糾紛。

經由上述國內外個資事故案件的分析我們可以發現，單單只是加強資訊安全上硬體及技術的投資，尚不足以安全的保護個人資料，還需要人員及流程上的妥善配合，才能有效的保護個資。

要達成這樣的目標，醫療院所、人力銀行及運輸旅宿等高風險的行業，可以考慮引入適當的個人資料保護與管理制度，透過制度建立的風險評估方法及不同層面的個資保護設計，來避免個資事故的風險；同時也正是因為資料的妥善管理與保護，才能因為了解資料的性質、脈絡、價值與限制，而妥善的將資料做有效的利用，讓這些產業的數位轉型（例如建立有效的數位化醫療環境等）有效的推動。

蘋果即時

上稿時間： 2020年10月29日

新聞來源： https://tw.appledaily.com/forum/20201029/TYPI3ZSSIJFN5JMXFNKWQRJ7IA/

文章標籤