資訊安全的新思維

◎魯明德

臺灣在過去數十年中，都是以高科技產業為發展的主流；然而，近年來服務業不斷興起，成為下一個新興的產業主流。高科技產業注重研發，擔心新研發的技術外流，且由於其技術層次高，因而可以了解並導入相關保密機制；而服務業則著重在服務的創新，其對高科技的技術應用層次相對較低，甚至對機密資料的敏感度，也較高科技產業低。

對機密資料的敏感度低，是不是表示服務業沒有機密資料？還是沒有人想要這些機密資料？小潘針對這個問題，上網爬文發現，其實在服務業中，也有不少洩密事件發生。例如：某銀行為避免員工監守自盜，在每台電腦上均裝有端點行為監測工具，用以監測員工的使用行為，惟該行襄理卻設法規避，並濫用自身權限去信用卡系統下載 20 萬筆客戶的個人資料，存放於私自加裝在公司電腦的硬碟中，再將附檔名更改為「mp3」，以避免被發現；事發後，該行控告該襄理妨害電腦使用罪。

看完這則報導，小潘基於職業敏感度，立刻心生疑問：這家銀行的監測系統為何如此容易被迴避？這樣的機制是不是會讓公司的機密資料很容易外洩？還是客戶的個人資料在銀行中不被認為是機密資料？

小潘把這些問題提出來，司馬特老師喝口咖啡緩緩道來：服務業者常常以為自己的技術獨特性不高而忽略保密作為，其實除了技術之外，服務業最大的資產應該是客戶的基本資料及消費資料，尤其是在海量資料（Big Data）下所獲取的資訊，更是服務業者賺錢的金雞母，不能等閒視之；從這個角度看，客戶資料被下載就不只是單純的刑法妨害電腦使用罪而已，在海量資料的架構下，客戶資料就不單純只是客戶資料，它可以為業者帶來客製化服務的效果，也可以擴大與競爭對手的差距，所以，它也是企業的營業秘密，適用《營業秘密法》的保護；同時，客戶資料又包含客戶的姓名、出生年月日、國民身分證統一編號、家庭、教育、職業、聯絡方式、財務情況等，得以直接或間接方式識別該個人之資料，所以它也是《個人資料保護法》所保護的範疇，資料一旦遭到洩漏，其所產生的損害，客戶也可以請求損害賠償，此舉將會造成企業的重大損失。

小潘聽完司馬特老師的說明才恍然大悟，原來服務業也是有它的機密資料，但是服務業在電子化之後，可以接觸到機密資料的人這麼多，該怎麼管理才不會造成機密的外洩呢？

司馬特老師繼續說下去：企業的資源有限，不可能無限制地投入在資訊安全上，而且服務業不像高科技產業，服務業的營運模式、客戶資料、消費模式等都是其營業秘密，在資源有限之下，主管部門就必須先確認對

企業營收影響最大的項目是什麼？**找到影響最大的點先做補強，而非從工程觀點出發，從最弱的資安環節開始補強**。

小潘聽完後開始迷糊了，因為一般在談到資訊安全的時候，都是從最弱的地方補強，為什麼老師要從對營收影響最大的地方著手呢？司馬特老師接續表示：**我們一直以來都認為資訊安全在防禦上需要成本，其實就攻擊方而言，駭客入侵也同樣需要成本**，如果在攻擊後所取得的效益小於攻擊所需耗費的資源，即使這些環節漏洞百出，也未必會遭到攻擊。在考量駭客的投資報酬率之後，企業的資訊部門就應該從企業的高度來評估，資訊系統遭到何種攻擊對企業營收的影響最深重？那一種攻擊對資訊系統而言，又是相對可以承受的？至於什麼是對企業營收影響最大的事，可能每個企業都不一樣；以前面的銀行案例而言，客戶的個人資料外洩，對公司所造成的損失比系統停機還要嚴重。但是，對於某些企業而言，則可能相反，如電力系統停機，對電力公司就是不可承受的痛。以前企業在建置資訊安全時，只考慮與駭客間的攻防問題，也就是外部存在哪些威脅，而企業又該如何防禦這些威脅。今天資訊主管必須考慮的，除了攻防之間的問題外，還要考量企業的營運面；也就是說，**企業在做資安決策時，必須更清楚知道哪些資料、哪些系統建置跟公司的營收相關性最大，從跟企業營收影響最大的地方著手**。

小潘想起上課時老師曾經提到，未來企業的資訊策略必須要引領企業策略，今天聽完司馬特老師的一番話，發現不只企業的資訊策略要跟企業策略結合，資訊安全的策略也要跟企業策略結合，才能確保影響企業營運的資訊不外洩。　（文摘自法務部調查局清流月刊 102 年 12 月號）

嘉義區監理所 關心您