資訊安全不可忽視的離職員工管理

作者：魯明德

報載聯發科的袁姓員工離職後，被公司查出在離職當日從公司配發的筆記型電腦裡重製了 2,053 筆資料，其中 208 筆是聯發科擁有著作財產權的資料，並將資料存在行動硬碟再帶離公司。袁姓員工則表示，離職時為進行工作交接，應其主管要求將資料複製下載至公司 IT 部門提供的行動硬碟，下載完後就將行動硬碟交給主管，並將電腦內資料清空交還給 IT 部門，帶離公司的部分是用個人隨身碟備份的個人資料。

從事資訊相關工作的科技新貴小潘也注意到這則新聞，於是他想到，如果這個情況發生在自己公司，該怎麼預防呢？在這個月的師生下午茶約會中，就跟司馬特老師提到這個新聞事件。

司馬特老師喝口咖啡緩緩地說，企業的資訊安全往往只注重員工在職期間的管理，機密資料不論是紙本及電子檔，企業都會對其訂出管理規定，要求在職員工要遵守，因此，洩密的風險尚在管控中。而對離職員工的管理相對就比較鬆散，風險往往由此而生。目前大多數的高科技公司都有資訊安全的意識，為防止內部機密資料外洩，通常都不會讓員工用自己的電腦從事公務，對於員工所配發的電腦，也會針對資訊安全，做些特殊處置，如控制 USB 的存取等措施，來防止員工擅自將檔案下載、外傳。但對於離職的員工，特別是高階主管，則往往變成資訊安全的死角。其實資訊安全應該是全體員工的責任，不只是資訊部門的責任。以這個案例而言，我們要思考的問題是：工作交接為何要把檔案複製到行動碟？主管為何要求離職員工將資料複製到行動碟？員工為何能備份自己的資料攜出公司？這些資料真的沒有公司的機密資料？

聽完司馬特老師提點的問題後，小潘接著問道：這些問題除了技術問題之外，應該還有管理問題吧！司馬特老師很高興小潘的舉一反三，喝口咖啡繼續說，在避免洩密的原則下，企業應對公用電腦的輸入／輸出做管制，坊間有很多現成的控制軟體可供選購，不用自行開發。透過控制軟體可以律定電腦的輸出／輸入權限，讓一般員工的電腦無法透過 USB 將資料匯出，以減少洩密的可能性。因業務需要而匯出資料時，則可做例外管理，經由資訊單位的設定，開放匯出資料，但系統仍須記錄匯出的內容，以做為事後追蹤之用。

小潘聽完後接著又問：人員離職要交接資料，電腦內的檔案如不匯出，如何交接？司馬特老師表示，離職人員業務的交接，如須交接電子檔案，可採取兩種措施：由於推行企業電子化，所以各公司都有內部網路，離職人員的電子檔案交接，可要求他放在公司的網路共用區內進行電子交換；如果公司沒有建立網路共用區的機制，或檔案有機密性，不適合放在共用區，則可由主管出面，協調資訊部門協助將檔案由離職人員的電腦中匯出，再匯入交接人員的電腦，處理完後，中介的行動碟內容立即銷毀，以避免機密資料外洩的風險。

小潘聽到這裏不禁產生疑問，司馬特老師看出小潘的疑惑，喝口咖啡繼續說，人員的離職原因百百種，不一定都會據實以告，有可能是要跳槽，所以竊取相關資料到新公司用，也有可能是挾怨報復，故意把重要的資料刪除，造成公司不可回復的損失。為了避免機密資料被故意或無意地刪除，對於離職人員的電腦，資訊部門應收回後再行處理為宜。誠如前述，資訊安全是全體員工的責任，因此，各級主管也要定期接受公司資訊安全的教育，了解公司對離職人員處理的標準作業程序，才不會下達錯誤的指示。其次，對於公司智慧財產權的管理，也和資訊安全密不可分，由於各企業多已電子化，當文件變成數位型態後，重製、散布相對比以前容易，所以規劃資訊安全管理制度時，要把智慧財產權的管理一併納入，包括數位版權管理的概念等都要在此時導入，讓員工即使把機密資料帶出，也無法打開來閱讀，讓公司的損失降低。

小潘聽完司馬特老師今天這一席話，對資訊安全又有了深一層的認識，原來資訊安全的範疇不只是對公司現有的員工管理，離職人員的管理更是重要；最容易疏忽的地方往往就是風險滋生的地方，真是不可輕忽啊！隨著華燈初上，小潘又帶著滿滿的收穫回到工作崗位上。

臺灣屏東地方法院檢察署關心您