清流月刊中華民國一百零四年八月號

「資料從公司寄到自己email算不算洩密？」寄的東西是否為機密文件，才是關鍵。

機密文件的管理

◎魯明德

報載台灣大哥大公司發現該公司管理手機經銷業務團隊及銷售手機予經銷商的經銷業務處副理，在離職前２天，利用公司電子郵件信箱，連續以附件形式，傳送有關銷售、通路展店、加盟店獎勵金等機密資訊，到公司外部的電子郵件信箱，遂以違反保密義務為由提出告訴，並要求依約賠償離職前半年的10倍平均月薪，約新台幣八十萬元。

經臺北地方法院審理後，法官認為他傳送的附件都屬簡報檔案，顯然是為多數人提供簡報而製作，內容並未註明或標示機密、限閱，且台灣大哥大又未舉證這些附件資料內容，已採取合理保密措施，難認定是契約所稱的機密資訊，因此，判決台灣大哥大敗訴。

企業在電子化後，幾乎所有的文件都變成數位資料並放在電腦上，科技新貴小潘看到了這則新聞，再加上記者聳動的標題：「資料寄到自己email不算洩密」，小潘開始擔心公司的機密資料，以後是不是都會用這種方式被洩漏？

小潘懷著忐忑不安的心情，終於等到這個月的師生下午茶約會，一見到司馬特老師就迫不及待把自己擔心好幾天的問題提出。司馬特老師看了小潘的剪報，維持其一貫的優雅態度，喝口咖啡娓娓道來，嚴格來說，記者下的標題並不對，「資料寄到自己email不算洩密」這個標題有點斷章取義。

其實這整個事件並不是自己寄信給自己就不算洩密的問題，記者下的這個標題不知道是無知還是看不懂判決書，還是故意想誤導大家，而是他所寄的內容並不是機密，如果他把公司的機密文件寄給自己，我想，法院還是會判他敗訴賠錢的。

小潘聽完立刻有了疑問，怎麼知道他寄的是不是機密資料？司馬特老師喝口咖啡繼續說，從剪報中很明顯的看出法官的心證，法官認為該員所傳送的檔案，並未註明或標示機密、限閱，且台灣大哥大又無法舉證，已對這些內容採取合理的保密措施。

所以，這整個問題的癥結就回到管理問題，從新聞剪報看起來，台灣大哥大應該是對其離職的副理提出侵害營業秘密之訴，而營業秘密的要件之一就是擁有營業秘密的人，必須要有合理的保密措施，否則就不構成營業秘密，既然所洩漏的不是營業秘密，也就沒有營業秘密侵害的問題了。

小潘聽到這裏立刻又有了疑問，什麼才是合理的保密措施？司馬特老師喝口咖啡接著說下去，合理是一個很抽象的概念，很難說要做到什麼程度才叫做合理，這要由法官來判斷。但是，企業一定要做到的是機密資料要有管理規定，將來到法院的訴訟才有可能勝訴。

最基本要做到的是在機密文件上一定要標示機密等級，如果文件上沒有任何機密等級的標示，拿到的人怎麼知道它是機密資料？怎麼知道要採取保密措施，讓無關的人不接觸它？在這個案子裏，法官也認為台灣大哥大並未在機密的文件上，註明或標示機密等級，這也是他敗訴的原因之一。

其次，企業應對內部的機密文件的管理，要訂出作業規範，並據以執行，例如，機密文件是如何產生的？應該透過那些程序產生？機密文件的保管、處理、歸檔、借閱…等，有沒有相關規定，這些都是合理的保密措施的一環。

如果公司宣稱的機密資料到處可見，都沒人管理，就會被認為是沒有管理，像可口可樂就號稱他們的營業秘密是鎖在銀行的保險箱中，而且要由公司的三個高階管理人員同時拿鑰匙去開，才能拿的到，這就是該公司對其營業秘密所採取的保密措施。

小潘聽到這裏，又有了新的問題，現在公司的資料都已數位化，放在內部網路上，要如何做到合理的保密措施？司馬特老師聽完了小潘的問題笑著說下去，數位資料可以透過加密、限制存取的方式，經由授權的管理程序，讓經過認證的使用者才能存取，即使合法的使用者把機密文件傳給無關人員，也會因為無法通過身分認證，而無法打開機密文件的檔案，而做到資訊安全的管控。

師生的下午茶約會，就在濃濃的焦糖瑪琪朵香味中進入尾聲，小潘聽完司馬特老師的一番說明，對機密文件的管理有了深一層的認知，心想，明天回到公司一定要對內部的機密文件管理重新檢視，對安全漏洞要及早補強。

（作者為科技大學資訊管理系講師）

▲Top

清流月刊 中華民國一百零四年八月號
機密外洩是導致作戰失利的關鍵，國內是否需禁止使用陸資的電信網路設備？

大陸電信設備龍頭「華為」引爆「婉君」攻防戰

◎楊俊彥

臺灣遭受網路攻擊密度是全球之冠，且駭客多數來自大陸，統計遭竊取資訊就已累積兩萬多筆；這對我國資訊安全帶來無形的威脅，其危險程度與大陸沿岸布署的飛彈不相上下。國內學者林穎佑（聖約翰科技大學教授）認為大陸除了成立網路戰部隊（簡稱網軍或婉君），更以商業為後盾支援網路戰，被點名企業如大陸華為。美國眾議院情報委員會曾對大陸華為進行調查，認為華為與大陸軍方有密切關聯，因此提醒美國企業不要與大陸華為合作。

調查顯示大陸華為是由退役的解放軍任正非上校於28年前（1987年）創辦，華為內部與大陸官方組織設有相對應的官職，也提供共軍網路戰部隊服務。華盛頓時報更報導華為於七年前接連三年（2008年至2011年）接受大陸政府（2.28億美金）70億臺幣的資助，且內部高層多人捲入賄賂疑雲，然而該公司最早的註冊資本額僅十萬臺幣，至近年卻成為全球第一大電信設備商，營收超越易利信。華為與大陸軍方異常金援關係，加上收受賄賂人員都可能是大陸網軍部隊的成員；因此國內的國安局明文規定電信業者不得採購陸資廠商的電信網路設備，國家通訊傳播委員會（NCC）與電信業者一直以來避免採購華為設備，這顯然受限於國家安全法。直至去年郭台銘的國碁電子進軍4G電信並擬採用華為網路設備，進而將反情報問題搬上檯面，假若臺灣的電信網路設備真使用華為的電信設備，那也就等同在臺灣本土安插了巨型木馬作為內應。

巨型木馬的典故源自希臘大軍久攻特洛伊城不下，於是將士兵藏於巨型木馬之中，當木馬被運進城中便伺機開城門引大軍。隨著駭客技術的發展，以前木馬是種電腦應用程式，而今早已進化成電路隱藏在電腦或網路設備之中，又稱木馬電路，使駭客輕易地進入系統，電腦使用者本身是無法發現，這種攻擊方式的人被稱為硬體駭客，且早已有先例可循，如大陸聯想電腦的所作所為。

大陸聯想在十年前（2005年）於大陸北京收購美國IBM個人電腦，事後經澳洲金融報導顯示，聯想電腦已被澳大利亞、美國、英國、加拿大、紐西蘭等五個國家的情報機構禁止使用。各國的實驗室測試顯示，聯想電腦設有內應，也就是木馬電路，可被他人在使用者不知情的情況下遠端操作。除此之外，英國和澳大利亞的多家情報和國防消息來源證實，存在一個書面禁令，禁止聯想電腦進入機密網路。禁令凸顯了對大陸公司生產電路中被植入木馬的擔憂，華盛頓布魯金斯學會的科技專家約翰教授表示，半導體市場的全球化使得晶片被惡意隱藏木馬電路插入供應鏈中。這些木馬電路可在數月或數年之後才變身成內應。高科技研究公司的資訊技術安全行銷分析師特納表示，木馬電路如果精心設計將很難被監測到，它們通常被設計得看起來像一個小的製造缺陷。加上今日技術電腦晶片製程已成長到奈米科技，根據牛頓時報形容，地球的奈米分之一大小相當於一顆彈珠，因此可以試想像一片指甲大小內擁有14億電晶體，經搭配網路通訊之後使駭客能輕易從遠端控制。木馬電路需要高度專業化的實驗室方能測試，大多數組織、企業沒有足夠的資源來監測這種木馬電路的滲入，所以聯想電腦遭多國機密網路禁用。

硬體駭客利用硬體電路，並可能對華為電信設備的電路做竄改，以達到植入木馬電路，一旦成功就可以逃避所有防火牆、防毒軟體以及安全輔助工具的追蹤，再次強調即便是電腦使用者本人（管理員）也根本不會察覺，除非電腦硬體損壞，否則此木馬電路將是一個永久的內應衛哨，供駭客隨意出入不做任何查緝，而且任何防駭措施對它也無濟於事。

商人往往看到的是利潤，郭台銘曾說：惡魔藏於細節裡。原意是用來提醒忽略細微處可導致嚴重失敗，亦可以解釋當你想做的事，困難的部分都是在很多小細節的地方，然而就我來看卻有另一層含意在其中，木馬電路小到你我看不見。未來的反情報戰已經非檯面化，基於所有資訊都網路化和數位化，加上兩岸開放自由行，華為的可攜式設備也早已慢慢地在自由的國土－臺灣銷售，禁止使用陸資電信核心設備將是固樁反制的積極作為。法國的國防承包商報告：因安全考量避免木馬電路作內應，華為被排除在澳大利亞國家寬頻網路之外。美國中央情報局更不諱言指控，華為是大陸的間諜。

「黃石公三略」所云：將謀洩則軍無勢，外窺內則禍不制。機密外洩導致作戰失利進而敗亡，絕無亡羊補牢的機會，若不慎遭敵人滲透，取得機密資訊，對國家造成的損害將無法彌補。根據《陸海空軍刑法》第63條第一項意圖損害軍事利益，非法輸出、干擾、變更、刪除軍事電磁紀錄，或以他法妨害其正確性者，處一年以上七年以下有期徒刑。

▲Top