清流月刊中華民國一百零二年十月號

企業的機密管理制度即使再周延完備，若是忽略對人的規範，也將會造成無法收拾的後果。

企業機密文件管理

◎魯明德

據報載國內某手機大廠的副總經理及其研發主管，將公司尚未上市的產品資料洩漏給競爭對手，被公司發現後提起告訴；渠等在檢調偵訊中還堅稱這些研發中的動物及人物的圖形介面等，都不屬於機密資料。

在科技公司上班的小潘看到這則新聞，立刻想到：同為科技研發公司，自己公司要如何防止類似的事件發生？機密資料要如何管理才不易外洩？

在例行的師生下午茶約會中，小潘迫不及待地把這個議題提出來。司馬特老師把這個問題分成二個層面回答：首先是文件的管理制度，其次是人員的管理制度。

《營業秘密法》在這次修訂後，已將刑責列入；營業秘密保護的要件有三：非一般涉及該類資訊之人所知悉者、因其秘密性而具有實際或潛在之經濟價值者、所有人已採取合理的保密措施。所以，保密措施將是影響營業秘密是否存在的一個關鍵因素。

從報導中發現，本案例中即使身為副總經理，都會辯稱不知道文件是具有機密性質，顯示公司在機密文件的管理上，可能沒有在文件上加以標示，以提醒使用者注意。當然，也有可能是副總經理的層級太高，反而成為保密環節中的漏網之魚。

在防止洩密的作為上，一定要先訂定各項機密等級制度，區分機密等級後，須在文件上標記，讓經手的人能夠注意。接著要去思考：如何讓該看到文件的人看到、不該看到文件的人無法看到，也就是要律訂何種層級之人，可以取得何種等級的機密文件。

其實組織內的洩密管道多如牛毛，根本之道就是如何讓適當的人知道適當的事，也就是need to know；但是，大多數的公司都是空有文件管理制度，卻是人人可以存取，並未達到管理的目的。

對於文件機密等級的運作原則，美國國防部發展出一套Bell-La Padula Model，其基本原則簡單地說，就是：No read up、No write down。除了對文件進行機密等級的劃分外，對人員同樣也律訂機密等級，所有文件的存取權限，必須依No read up、No write down的原則進行。No read up是指不允許閱讀高於本身機密等級的文件，以免文件讓不應知悉的人員知道。No write down則是不允許寫出低於本身機密等級的文件，以避免承辦人因為在撰寫較自己機密等級低的文件時，有意或無意間將知悉的機密資訊寫入，造成洩密事件。

人是組織中知識或技術的產生者，同時也是造成洩密事件的始作俑者；所以，組織除了要有健全的文件管理制度外，還要對相關人員加以管理。人員的管理包括公司內部的正式人員、外包人員、協力廠商等。企業對公司內部的正式人員大多會有相關規定，但往往忽略外包人員及協力廠商等；對於外包人員也應律訂機密等級，使其僅能接觸與他的機密等級相同的文件；對於協力廠商的人員管理，則應先與協力廠簽訂保密協定，並要求廠商亦須與其員工簽訂相同的協定，由廠商與員工共負洩密責任；另外，員工的流動也是造成機密外洩的主要因素之一，尤其是核心成員帶著關鍵技術跳槽到競爭對手或自立門戶，都會對原組織造成重大的傷害，所以也要嚴加防範。

為防止類似事件，除了文件的管理外，相關保密的教育訓練也很重要，並且要持續進行。在人力資源管理上，對於新進人員要請他簽訂保密合約，以約束其行為，事先防範其在職期間違反規定。當員工離職時，尤其是關鍵人員離職時，一定要透過離職面談告知其應負的保密責任，以避免渠等將機密資訊帶往對手陣營。

最後，還有三個族群是組織在保密上容易疏忽的，他們是最容易洩密卻又不受拘束的高風險群，其分別是：清潔外包人員、文件收發傳遞人員、高階主管。清潔人員可以透過與清潔公司的合約加以約束，文件收發傳遞人員可以由員工守則予以規範，最危險的就是高階主管，通常大家對長官較無戒心，且懾於其職權，幾乎都是有求必應，如果他有異心，可能就會是最大的炸彈，如前述案例一般。

小潘聽完司馬特老師的一番話，對企業的保密作為有了更深一層的認識，心想：人的管理還是最難的一環，即使制度設計得再周延，高階人員如果有心想做壞事，還真難加以防範啊！

（作者為科技大學資訊管理系講師）

▲Top

清流月刊中華民國一百零二年十月號

資訊擁有者、使用者與雲端平臺管理員都應了解網路攻擊的趨勢，只有掌握最新的雲端威脅，才能確保資訊服務的安全。

認識雲端服務與安全

◎李柏毅

雲端服務是一個大家目前耳熟能詳的網路名詞。這一朵原本只存在網路拓樸圖上的雲，隨著資訊科技的不斷進步與革新，已經慢慢地擴大到我們每一個人的日常生活中了。

雲端服務（Cloud Service）是一項結合雲端運算（Cloud Computing）、雲端儲存（Cloud Storage）、網路連線與管理的新時代網際網路服務。國際研究暨顧問機構Gartner對雲端服務的註解為：雲端服務是大量且具有可擴充性的資訊資源，透過網路以服務的方式提供給使用者存取。舉凡影音娛樂、文書處理、收發電子郵件、訊息交換、瀏覽網頁等日常的網路行為，以至於醫療機構為居家照護患者所提供的遠端醫療服務、教育機構的遠距教學平臺等公共服務，都在雲端服務的範疇之中。

美國國家技術標準局提出雲端服務應具備的五種性質：

一、隨需自助服務：在使用者需要雲端服務時，可在不透過其他系統維運人員的協助之下，於任何時候自行存取所需要的服務內容。如此一來，雲端服務就能協助企業或組織提升服務效率，增加使用者的滿意度，同時也可以降低互動時間以及服務成本。

二、網路服務連線：由於網際網路技術的進步和無線網路建設的普及，雲端服務已能讓使用者在地球上任何一個角落，透過網路通訊標準進行服務存取。

三、資源共享：透過虛擬化及其他綠能科技的協助，雲端服務可同時將運算和儲存資源分享給許多使用者，如此一來，即可大量減少硬體閒置資源的浪費，也可透過專業化的集中管理，降低服務成本。

四、彈性部署：可彈性化部署的伺服器群以及網路儲存設備提供了雲端服務高度的服務彈性化，使用者可以依據自己的需求，進行服務的增加、刪除。

五、量化服務：雲端服務可以根據資源的使用，進行量化指標的監控，包含CPU數目、記憶體使用量、儲存空間的使用量、網路頻寬的使用量等；這樣的特色有助於幫助管理員監控服務的即時狀態，也能針對各種服務的使用狀況進行資源最佳化的分配。

當雲端服務越來越普及時，其所衍生的資安問題將會是下一波被大家重視的課題。謹就雲端安全聯盟（Cloud Security Alliance）提出的七大雲端威脅分述如下：

一、雲端運算的濫用：資訊的進步除了提供使用者更便利的生活，同時也會造成新的資安問題。近年來越來越多的網路犯罪者已開始透過雲端服務來進行不法行為。例如利用殭屍網路（Botnet）作為訊息交換的中繼站，建構在雲端服務商所提供的系統平臺上，藉由正常雲端服務的網路流量，隱藏殭屍電腦的通訊行為，並躲過偵查。此外，雲端運算也已被利用來提供密碼破解的服務，只要有心人士取得系統的帳號密碼資料檔案，並將其中的MD5雜湊值（Hash value）取出，透過現成的雲端服務，即可分析出該雜湊值所代表的可能密碼組合，進而取得系統內部的任何帳號密碼。

二、不安全的通訊介面或是應用程式：使用者使用特定的通訊介面與應用程式存取雲端服務，因此，當通訊介面或是應用程式發生安全漏洞時，都會影響服務存取的安全，造成資料在未經授權的狀況下，遭到第三人存取或是修改。

三、內鬼難防：當所有的資訊服務都移轉到雲端空間時，管理的責任同時也部分移轉到雲端服務供應商身上。因此，若雲端服務供應商內部存有居心不良的使用者，便可能對存放在雲端服務平臺的資訊造成危害。這方面的風險，是使用者無法預測與轉嫁的。

四、資源共享造成的潛在問題：資源共享雖可節省閒置資源的浪費，達到節能省碳的目的，但同時也衍生資料保密的問題。雲端服務使用虛擬化的技術，將實體的資訊資源同時分配給多位使用者存取，雖然每一位使用者都是使用獨立的運算空間，但若其實體隔離機制出現漏洞，有心人士確實可以藉此影響其他雲端服務，甚至讀取其記憶體或是儲存空間的資料。

五、檔案遺失或資料外洩：雲端服務供應商在資料保全上所提供的安全防護機制，也必須要能確保使用者的資料不會受到未經授權的存取；若發生資料毀損的狀況時，雲端服務供應商也必須要有完善的資料備援機制，才能降低資料遺失的風險。

六、帳號或服務挾持：雲端服務的認證機制主要係透過網際網路的方式，藉由輸入帳號密碼來進行身分確認。一旦使用者帳號遭到竊取或是資訊傳輸的過程，連線遭到中間人攻擊重設，都會導致第三者取代原使用者而取得該系統的完整控制權。由於使用者無法透過重設實體系統（本機終端機登入或是切斷網路連線）來進行緊急應變，所以一旦帳號密碼外洩或是服務被挾持了，其損害程度及影響範圍可說是無法評估。

七、未知風險：雲端服務隨著資訊科技的進步，也在不斷地改變其服務型態，所以未知的困難以及可預見的資安問題將會越來越多。

雲端服務改變了以往資訊服務的面貌。透過網路，使用者可以隨心所欲地使用雲端資源，組織單位也可以透過雲端服務，降低服務建置與管理成本。但隨著服務型態改變所衍生的資安問題，並不會同時全部移轉到雲端服務提供者身上，凡是資訊擁有者、使用者與雲端平臺管理員都必須了解網路攻擊的趨勢，掌握最新的雲端威脅，才能確保資訊服務的安全。

（作者為國家實驗研究院國家高速網路與計算機中心網路與資安組助理工程師）

▲Top