機密資料流通的管理，應從紙本及數位文件二方面同時著手，並訂定相關的管理規範，才能有效防堵資安漏洞。

機密資料流通的管理

◎魯明德

小潘任職的高科技公司，在資訊安全技術研發上已有相當的成果。某日小潘發現市面上的競爭對手疑似採用相同的技術，經過內部檢討後，發現該項技術可能是被前來洽公的客戶順手攜出。公司發現如此重大的資安漏洞，立即要求研發部採取補救措施，以遏止機密資料繼續外洩。小潘接到任務後不知從何下手，於是趕緊求助司馬特老師。

在例行的下午茶約會中，小潘一見到司馬特老師，立刻將他面臨的問題提出來。老師聽完後提了一個問題：「你認為機密資料包括那些？」小潘想了一會兒，回答說：「應該包括紙本的文件和數位化的檔案或文件」。司馬特老師點頭嘉許小潘對資訊安全已有初步概念，接著就從這兩方面來說明。

對於機密資料的管理，應從紙本文件及數位文件二方面同時著手，才不會造成危安因子。就紙本文件而言，機密文件除了須標示機密等級外，還要律訂保密期限，並造冊列管、定期清點；分發時也要編號造冊，由接收單位或個人簽收，才能管制機密文件的流向，將來萬一流失，才能根據文件上的編號追蹤流失來源，採取補救措施。

由於機密文件涉及研發技術，不可能每天鎖在櫃子不用，所以對於機密文件的流通也要訂定相關規範。例如機密資料的外借必須確實登記，且借閱訂有期限，屆期就要催還，以免日久佚失。

小潘又想到另外一個問題，機密資料失效後要怎麼辦？司馬特老師邊喝咖啡邊點頭，讚許小潘的舉一反三。

機密資料都訂有保密期限，屆期就要予以銷毀，通常都以水銷或碎紙機將其攪碎再回收。小潘聽到這裏又開始納悶了，對於技術性文件，都是公司努力研發得來的成果，若就此銷毀，豈不可惜？

老師解釋說，對於研發成果當然不能隨便銷毀，保密期限到了就可公開給公司的研發人員做為教育訓練之用，讓員工知道技術的原理，以使知識傳承下去。但首先要做解密作業，因此，公司也要訂定機密資料的解密作業程序，將解密後的技術資料納入管理。

小潘接著問，對於數位化的文件，我們又該怎麼管理呢？老師繼續說道，數位化的文件或檔案，通常置於公司內部的公用網路上，公用區最基本的安全規範，就是每個資料夾都要設定存取權限，以防止不必要的人接觸到機密資料。聽到這裏，小潘又問：如果有存取權限的人，把資料傳給沒有權限的人，而使機密資料散布出去，該怎麼辦？

司馬特老師繼續說明，要防止合法接觸機密文件的人，隨意散布機密文件，可利用資訊科技來做管理，例如：數位版權管理(Digital Right Management），它使用加密演算法，透過憑證管理來做權限管理。系統可以先定義每位同仁的機密等級，對於已經核定機密等級的文件，在開啟前，系統就會先藉由憑證來驗證使用者的身分，確認他是合法的使用者；接著核對開啟檔案的人是否符合該機密等級，如果機密等級不夠，則系統不會讓他開啟檔案。因此，即使是具有權限的合法使用者把機密檔案轉給沒有權限的使用者，系統會發現他的機密等級不夠，就無法開啟機密文件的檔案，自然可以防止機密資料隨意散布的問題。

小潘又問道，機密文件寄給機密等級不夠的人，對方雖然看不到，但有沒有可能由合法使用者列印出來，或把它複製到 word 檔上再加以散布？要如何預防呢？

司馬特老師喝完最後一口咖啡說道，這也可以透過數位版權管理來控制，系統可以把列為機密等級以上的文件，將它的列印與複製的功能拿掉，以控制它不能被列印，也不能被複製，確保機密文件不會外洩。

小潘經過司馬特老師一下午的詳細解說，對於紙本文件的保密作為及數位版權管理有了新的認識；心想今晚應該要趁著記憶猶新的時候，趕快把機密文件的管理程序寫出來，以補救公司的資安漏洞。