工作效率與資通訊安全的衡平

◎魯明德

隨著資訊科技的匯流，企業在談資訊安全時，不能再只偏重資訊科技；在網網相連的環境中，通訊已是不可或缺的資訊傳遞載具，因此，通訊設備的安全也要一併納入考量與規劃，資訊安全才不會有死角。

繼蘋果的雲端造成隱私外洩事件後，蘋果的 iPhone 及小米的手機都陸續傳出手機在使用時，會自動把使用者放在手機上的資料，回傳到自己連結的伺服器上，造成使用者人人自危。無獨有偶，立法委員也在立法院點起 Line 資安疑慮之火，行政院並發出公文，要求各公務機關禁止用 Line 連絡公務。

科技新貴小潘看到最近的這些新聞，不禁懷疑：科技的運用，不就是要用來提升工作效率的嗎？有資安疑慮就停用，這不是因噎廢食嗎？自己的公司自從推動電子化，所有的設計資料、庫存資料、客戶資料等都放在網路上，要怎麼做才能確保安全呢？

在這個月的師生下午茶約會中，小潘就迫不及待地把問題提出來。司馬特老師喝口咖啡，隨口問了小潘幾個問題：你們公司放在網路上的資料都是什麼資料？有沒有做什麼安全管制？你們在 Line 群組上談的是什麼？傳送的資料又是什麼？

對於司馬特老師所提的問題，小潘想了一下表示：公司放在網路上的資料包羅萬象，從研發、財務、人事、行銷等，甚至於福委會的特約商店資料，全都放在網路上，這要怎麼管理？

司馬特老師聽完，笑著說道：這麼多的資料放在網路上，是不是應該分類管理呢？把網路和資料都分為兩部分，網路分為內部網路與外部網路兩個獨立的部分，將需要提供員工透過網際網路存取的資料，置於外部網路，不提供員工從網際網路存取的資料，放在內部網路。除了內部網路要做資安管理外，外部網路更要進行資安管理，可以設置虛擬私有網路的方式提供員工存取，當然，權限管理、防火牆等都是不可或缺的。在內容上，也要做篩選，不是所有的資料都可放在外部網路上供人存取，因此，第一步要做的就是內容分級，公司要先定義機密等級，再依機密等級的定義，對文件進行分類。第二步就是對人員進行機密等級的分類，員工只能依照所賦予的機密等級，存取符合的資訊。

小潘聽到這裏，又有一個疑問，員工的機密等級應該怎麼訂呢？司馬特老師喝口咖啡，緩緩地說：員工機密等級的訂定，只要符合 need to know 的原則就可以，也就是員工只要知道他該知道的就可以了。機密等級分類

完成後，就要檢討哪些資料是工作上需要，必須放在外部網路讓員工透過網路存取；這些資料獨立以鏡射（mirror site）的方式，置於獨立的外部網路上，這樣做的好處是即使外部網站遭到攻擊，也不會影響內部的資料安全，攻擊後的修復程序也比較單純。置於外部網路上的資料，因為已做過機密等級的分類，對於具有機密性的資料，則以加密方式處理，員工有權限者才能打開讀取，所以即使被攻擊，攻擊者也無法輕易知道內容，可以增加資料的安全性。

對於加密的工具，一般企業不需要花錢自行開發，坊間有很多文件管理的套裝軟體，都能提供相關功能，只要花時間去評估一個適用的即可。

小潘聽完司馬特老師的說明，對於資料的安全管理有了新的認識；接著又問到：Line 是目前國內最常使用的一種社群 APP，任何的通訊軟體它們會在背後做些什麼事，使用者是不易得知的；社群 APP 要傳送訊息時，本來就要透過伺服器，而伺服器端會做什麼事，則不是我們使用者可以控制的，難道我們只有禁用一途嗎？

司馬特老師喝口咖啡，以悠閒的語氣回答著：水能載舟、亦能覆舟，難道擔心船會翻，就不坐船了嗎？回到前面所說的，如果公司已經把文件、人員都做了機密等級的分類，就要嚴格落實人員的資訊安全管理與教育，對於具有機密等級的資訊，不可以透過 Line 來傳送，這個傳送包括檔案的傳送及群組訊息的廣播。檔案的傳送必須要與公司的資安作為配合，因為內部網路是一個獨立的網路，它的資料匯出就要管制，不能隨便匯出到行動裝置，這樣檔案才不會經由 Line 傳送出去，而且機密資料的儲存，一定要經過加密處理，即使第一線失守，取得資料的人也不會這麼容易就開啟。

經過一下午與司馬特老師的討論，小潘心中有了領悟，資訊科技是用來提升工作效率的工具，資訊匯流是一個不能回頭的潮流，企業不能自絕其外；而資訊安全就像大禹治水一樣，一味地害怕、防堵是沒有用的。在這股資訊匯流的趨勢裡，我們要學著運用管理及科技來確保公司裏的資訊安全，才是正確的路。

這個月的師生約會，就在華燈初上伴著焦糖瑪奇朵的香味中進入尾聲，小潘經過一下午的充電，帶著滿滿的收穫回到工作崗位上，也期待著下一次的下午茶約會。（文摘自法務部調查局清流月刊 103 年 11 月號）

嘉義區監理所 關心您