

「智慧財產權專欄」系列二十五

標題：企業經營者如何避免因軟體管理疏失而導致的經營風險(下篇)

就企業內部自行開發之軟體或是具有商業價值的資訊而言，由於電腦及網路的快速發展與普及，企業內部資訊遭到竊取的事件層出不窮，而就我國現行的法律規範而言，對於竊取公司營業上機密或離職員工違反競業禁止之契約義務時，民事責任方面權利人可以主張侵權行為、違反契約義務或主張營業秘密法來請求賠償，然實質上法律對於各種請求權仍有一定的要件限制(例如：營業秘密其「秘密性」必須具有實際或潛在之經濟價值；且所有人已採取適當之保密措施者)。雖法律的救濟有其實益，但是如果機密的資訊一旦外洩，縱使歷經長年的訴訟而獲致勝訴判決，其對於企業而言意義也可能已經不大。因此與其消極的等待法律的保護，不如積極的建立一個完善的資訊管理制度，提供事前的防範。

目前企業界對於防止自家營業上之資訊外洩，多半會與員工簽訂保密合約，然而保密合約的簽署所能達到的效果有限，屆時資訊外洩時，公司仍須負舉證責任，具體指出契約所指的機密為何，而相對人確實洩漏了其中的秘密，違反了契約義務等事實。因此除了一紙保密契約外，公司應事先將秘密的範圍界定清楚，使員工確實知悉其義務範圍。另外在形式上，公司內部也應採取若干保密措施以維護前述機密，以免將來對保護標的的「秘密性」有所爭議。另外，合理的離職後競業禁止條款，也可以考慮一併納入，當然也必須兼顧員工依據憲法的工作權。

一般來說，目前許多企業之內部資訊或軟體的管理方式係採取集中式的管理，例如由專職的資訊部門人員負責或成立單一的資料中心來控管。但實務上卻發現，由資訊部門人員來擔任管理的工作，可能會因為資訊人員對於公司各組織之運作不甚熟悉，或人員編制過少，未能發揮如期的效果。因此，建議對於內部資訊與軟體資料的管理，不應只是某個部門或少數人的責任，而應該分別於適當的層級上建立控制點。建議可考慮以下幾點：執行者與覆核者不應為同一人、相關軟體及資訊應適當的分級管理、相關的管理措施應留下審計軌跡。控制點的建立可以有效的監控，但應注意分級之適當與否，以避免造成過與不及，亦不至於影響經營效率。另可委託獨立的機構或有經驗的風險管理顧問公司進行定期或不定期的稽核，如此一來，可以藉由一個獨立且客觀的第三者將公司內部的控制串接成一個有效率而又有外律機制的管理制度。

企業經營者若忽視企業內部軟體使用的管理，非法使用軟體，可能招致民、刑事的法律究責，產生巨額的罰金損失，嚴重影響企業競爭力與形象。而對於企業自行開發具有商業價值的資訊或軟體而言，對於企業經營損失之影響更是無法估計。在中小企業林立的我國，建議企業經營者應不分企業的規模大小，積極建立智慧財產權管理制度，消極的避免侵害他人的智慧財產權，積極的創造、累積自己的智慧財產權，從經營上做全方位考量，在成本與風險考量上取得平衡點，以取得營運效果的最大值。

(本文作者為台灣商業軟體聯盟)