智慧財產權風險——營業秘密

林鴻諭 Aon 金融服務暨專業險部 協理
魏于華 Aon 金融服務暨專業險部 專員

林鴻諭 協理

在1975 年，S&P 500 指數中市值最大的前五家公司分別是：IBM、ExxonMobil、P&G、GE 和 3M，而到了 2018 年則是 Apple、Microsoft、Amazon、Facebook 和 Alphabet，都是一些掌握著大量無形資產的企業。

2018 年無形資產占 S&P 500 指數價值的 84%，約 19 兆美元，已然成為創造企業價值的主要原動力。

智慧財產權是構建企業競爭力的重要成分。智慧財產權包含對研發的投資，以及對軟硬體設備、材料、製程和設計等投入。在今日智慧財產權已成為決定企業競爭優勢和經營成敗的關鍵因素之一，對企業來說，理解智慧財產權如何影響企業長期成長動能以及經營風險是至關重要的。智慧財產權包含專利權、商標權、著作權與營業秘密等項目，其中「營業秘密」近年特別受到關注，營業秘密的主要優點是，企業不需要對外揭露具體細節，這提供了企業更好的保護，且營業秘密沒有期限限制。營業秘密被認為是數位經濟的真正主力，但因為營業秘密本身的特殊性質，人們對營業秘密在市場競爭中的作用瞭解遠遠少於專利、版權和商標。

然而在近年來數位科技的進步下，營業秘密變得更容易散播或存取，整體管理難度也隨之上升，再加上公司離職員工帶走營業秘密投靠競爭對手的新聞事件層出不窮，企業紛紛意識到營業秘密被竊或侵害的嚴重性，**畢竟營業秘密是能夠為企業帶來獲利的關鍵動力，若這些營業秘密被競爭對手取得，對企業所造成的傷害將難以輕易消弭。**

台灣晶圓代工大廠因員工攜帶前公司機敏資訊投入工作中，而遭美國記憶體大廠指控竊取營業秘密，纏訟多年後，最後，該晶圓代工大廠最後同意與美國司法部進行認罪協商，達成和解並支付 6000 萬美元之罰款，台灣地方法院亦判處 1 億罰金，付出不小代價。類似的商業機密盜取案例，在日前也發生在台灣的電動機車產業中，一知名電動機車大廠發現競爭對手開發之電池與其技術規格相似度高，懷疑機密技術遭竊，檢調獲報後展開追查搜索及約談相關人士，相關涉案人士也遭羈押。

依照營業秘密法規定，須符合**「秘密性、經濟價值性、合理保密措施」**三要件才可被視為營業秘密而受到營業秘密法保護。然而在許多實際案例中可以

發現，此三要件並非容易符合，勝訴率更是低落，主要是因為企業對於營業秘密缺乏明確定義及留下管理軌跡證據，在訴訟時無法提出有力證明，因而難以達成保護企業機密資訊的目的。

營業秘密三要件

- **秘密性** 指必須是他人難以得知的資訊，若是可透過網路查詢得知，或在業界廣受他人認知之資訊，則不屬於營業秘密的範疇，惟進行訴訟時該資訊是否具備秘密性且為原告所獨有，仍須由原告負舉證之責，證明該資訊並非他方所知悉。此外，企業內部常見之營業秘密，可大致區分為兩類「商業性營業秘密」及「技術性營業秘密」，前者包含客戶名單、定價策略、成本、人事管理等企業營運相關資訊。這類資訊是否具備秘密性，應視其是否能夠從公開管道獲取，或是否需要額外投入精力進行整理、分析，使之成為營運時可使用之重要資訊。而「技術性營業秘密」則包括產品生產方法、技術、製程與配方等與企業研發或技術創新有關之機密資訊，有關此等資訊是否只專屬於特定公司所擁有，須由主張該技術性資訊為營業秘密之企業負舉證之責任。

- **經濟價值** 該資訊因其秘密性而能夠幫助企業產出經濟利益或商業價值。評估是否具備經濟性之重點包含研發的成本投入、影響企業競爭力、市占率或造成銷售額之減損，與影響未來收益等。

- **合理保密措施** 企業應採取合理必要之保密措施，使他人了解其對營業秘密有加以保密之意願，而在實際上採取積極作為對營業秘密進行保護。例如針對電腦資訊設定使用者權限、防火牆、密碼登入等，或是對相關機密文件予以上鎖、限制訪客等。

營業秘密風險管理

如何管理營業秘密，相信是各企業皆非常關注之議題。建立一個完整的營業祕密管理機制，應包含「事前預防」及「事後應變」。

事前預防

- **盤點機密資訊** 管理制度的建立首先需要企業高層的支持及明確政策方針、指示，以為進行營業秘密管理所生必要之時間、成本投入提供支援。再來則是辨認出企業有哪些營業祕密，可以透過盤點機密資訊，分類分級與標示，來區分何者才是支持企業營運不可或缺的重要核心。

- **適當保護** 分析既有的業務流程，將機密資訊辨識與標示清楚，同時針對攜出、複製、重製進行控管審核，並確保留存足夠的管理紀錄軌跡，即時掌握營業秘密之流向以防堵缺口。營業秘密除須妥善保存外，在資訊生命週期尾聲回收銷毀機制也同等重要，錯誤的處置將提升營業秘密外洩風險。另外，存放營業秘密之場所也須有進出入管制或保全設置，將之與一般營業場所區隔開以降低外洩風險。資訊時代下電腦系統安全管理也不容輕忽，加密限制、網路連線認證或防火牆等，皆是重點防禦之處。

- **人員管理** 人才流動是企業營運不可避免的，每當有員工加入或離去，可能或多或少地增加企業營業祕密外洩的風險，企業高層須正視人員管理，在員工離職時，可進行離職面談，重申該離職員工應負之保密義務，並確認其是否仍持有公司的營業秘密資訊，離職面談也有助於企業取得將來發生訴訟時可能有幫助的佐證資料，釐清離職員工接觸或使用之營業秘密範圍，將有助於提

高未來潛在訴訟之成功率，及減少舉證難度與訴訟費用。至於針對聘任新員工則須注意其與前僱主間之營業秘密風險，主動採取更積極之控管手段。透過僱傭契約、教育訓練、員工守則等，培養並規範員工職業道德，適時地與員工簽訂保密及競業禁止條款，皆是企業可以納入人員管理的措施。

事後應變

企業在日常便需建立**危機應變計畫流程**，以在營業秘密不幸外流的狀況下能迅速作出回應，降低對企業營運的損失及傷害，並可適時結合外部專家、顧問對法律諮詢、證據保存及鑑識提供協助。切勿等到事發後才開始檢討如何保護企業營業秘密，錯過危機處理的黃金時機，將對企業帶來龐大的衝擊。

全球化浪潮來襲，資金、技術、人才的跨國流動更為頻繁，企業間的競爭也越趨激烈，我們不乏聽聞各種商業間諜或是營業秘密盜竊事件發生，且當今中美貿易戰持續進行，智慧財產權更是雙方爭議重點。企業在面臨如此環境下，更應重視營業秘密的保護，企業應充分理解營業秘密之戰略價值，並妥善規劃控管流程、提升資訊安全性，在營業秘密被竊取時，更應做出危機應變，主動提出訴訟以捍衛企業核心價值，確保競爭力，並透過保險降低訴訟帶來的鉅額損失，為股東權益作出貢獻。