企業資安管理重中之重

工商時報名家廣場-2024.03.07

文 / 黃譯漫 證券暨期貨市場發展基金會助理研究員

隨著遠端工作、異地辦公之工作新型態的普及，加上行動支付、雲端計算等技術革新，人類生活與企業營運愈發仰賴網路，但接踵而至的是資訊安全相關的違法事件與相關風險。安侯建業會計師事務所（KPMG）於今年 1 月發布「2023 年全球與台灣 CEO 觀點及趨勢摘要」，闡明台灣 CEO 認為影響企業之前五大風險，第一是「企業營運風險」，其次「監管法規風險」與「新興/顛覆性科技風險」併列第二，「數位網路安全」、「供應鏈風險」及「利率風險」等。

新興/顛覆性科技風險、網路安全，考驗企業營運

前述風險在講究內部控制與流程的企業營運中，可看出在科技進步伴隨相關營運風險增加的同時，資安管理成為重中之重。

為提升公開發行公司對資安之重視， 2021 年 12 月我國金融監督管理委員會（下稱金管會）於新版「公開發行公司建立內部控制制度處理準則」新增第 9 條之 1，規範企業必須配置適當人力資源與設備，進行資安制度之規劃、監控及執行資安管理作業。另外，若符合一定

條件者，即有關公開發行公司應指派資訊安全長及設置資訊安全專責單位之一定條件，授權主管機關另定之外，金管會得命令指派綜理資安政策推動及資源調度事務之人兼任資訊安全長，及設置資訊安全專責單位、主管及人員。

賡續強化企業資通安全機制，金管會於 2023 年 3 月以「資訊揭露」、「公司治理」及「監理協助」等三大面向積極推動資安管理措施。其中，「資訊揭露」著重企業若發生重大資安事件須及時發布重訊，並於年報及公開說明書敘明資通安全管理政策與方案、投入資源、資安風險影響程度等，及所遭受重大資通安全事件之影響；「公司治理」則為金管會依資本額規模、市值、業務性質及營運狀況等將上市櫃公司劃分為 3 等級，並分階段要求企業配置資安人力資源，且證交所與櫃買中心訂定資通安全管控指引，以提供企業完善資安防護措施及管理機制；至於「監理角度」，金管會鼓勵企業依風險等級加入台灣電腦網路危機處理暨協調中心（TWCERT）共享資訊安全情資，並鼓勵企業導入 ISO 27001、CNS 27001 等資訊安全管理系統標準，或取得第三方驗證標準。有關導入資訊安全管理系統標準，亦納入公司治理評鑑指標加分題項，期導引資通安全管理於公司治理文化。

國內外強化管理規範 助企業控管資安

因應網路安全與風險管理之議題，美國證券管理委員會於 2023 年 7 月通過上市公司實施網路安全事件與風險監督流程揭露義務之新規則，包括於 Form 8-K 重大訊息報告中，當重大網路安全事件發生後四個工作日內，須揭露相關重大資訊，並於同年 12 月 18 日起實施。

另外，SEC 也要求企業於 Form 10-K 年度報告須揭露網路安全流程和監督等內容，包含「評估、識別及管理網路安全威脅風險的企業流程」、「已對企業產生重大影響，或可能產生重大影響之網路安全威脅風險」、「董事會對網路安全之監督，及負責監督之小組組織」，與「管理階層評估或管理網路安全威脅之功用，包括管理階層的職級及相關專業知識之描述」。

綜上，不論國內外，資訊安全相關重大事件之事前風險評估、事發因應措施，及事後之重訊揭露，儼然成為政策推動的核心。如此不僅能提升企業資安意識，亦可強化外部投資人對企業之信心，使得利害關係人受有保障。

借鏡國際趨勢及我國政策之推動，企業營運不可忽視資訊安全管理，甚至資訊安全必須成為公司治理著重面向之一，讓資安管理恪守最後

一道防線，使企業若不幸曝險於資安危機時，仍具有相當韌性與因應措施可應對，進而提升投資人信心。