美國：企業加速揭露減緩網路風險之措施

美國證管會（SEC）7 月要求上市公司每年揭露網路安全風險管理策略、治理措施及任何重大網路安全事件的規定，ISS 針對美國公司揭露網路安全風險監督措施進行分析並發布報告。報告結果顯示，在 SEC 規定生效前，企業正努力向利害關係人說明企業擁有管理網路安全威脅的有效方法。此外，分析發現幾乎所有 Russell 3000 指數公司都揭露包括減緩公司資訊安全風險方法之資訊，其中一半以上的公司還詳細揭露資訊安全風險及緩解風險的策略或計畫。在 S&P500 指數中，80% 以上公司揭露有關風險和減緩方法的詳細資訊。

此外，愈來愈多企業詳細說明資訊安全培訓計畫，在過去兩年中 S&P500 公司增加近 55%，Russell 3000 指數（不含 S&P500 指數）公司增加 100%。截至 2023 年 9 月，近 67%S&P500 指數公司與 57%Russell 3000 指數公司（不含 S&P500 指數）揭露資訊安全風險保險政策之企業數量亦於同期上升。

網路安全風險監督已成為董事會層面關注的問題，愈來愈多公司正要求董事具備應對挑戰所需之專業知識。雖然 SEC 規定之最終版本排除董事會明確揭露董事網路相關專業知識的要求，但許多投資人意識到基於股東利益，董事有責任在資訊安全監督方面盡責；而擁有相關知能之董事則向投資人表示，董事會具備有效監督網路安全風險所需的專業知識。此外，具有資訊安全專業知識的董事在大型公司更為常見，S&P500 指數公司中超過一半的公司至少有 3 名具有相關專業知識的董事。然而，在 Russell 3000 指數（不含 S&P500 指數）中，超過 40% 公司未揭露有任何具備網路安全專業知識的董事，僅約 20% 公司擁有 3 名以上具備此類技能的董事。而少數公司（16 家 S&P500 指數公司和 22 家 Russell 3000 指數公司（不含 S&P500 指數））將網路安全措施作為年度，或長期高階薪酬激勵計畫之一部分。

ISS Corporate Solutions 常務董事兼網路策略主管 Doug Clare 表示，SEC 新的網路揭露規則對管理團隊與董事會而言，係一項強制職能。由於企業現在需要對其網路風險管理加強揭露，這些規則無疑將迫使許多公司採用更有力的流程，以滿足揭露的要求。

（資料來源：美國企業加速揭露緩解網路風險之措施，2023 年 9 月 19 日，https://insights.issgovernance.com/posts/u-s-companies-step-up-cyber-risk-mitigation-disclosures-in-advance-of-forthcoming-sec-requirements/ ）