美國：企業必須公布網路攻擊情況

據估計網路間諜及竊盜每年從美國公司盜取數百億美元價值的資料。但是專家說很少有公司會向股東報告相關損失。

現在美國證券交易委員會（Securities and Exchange Commission，SEC）將要求增加揭露此類事件，並於本週簽署新的指導準則清楚規定公開上市公司必須公布其遭受重大的網路竊盜、網路攻擊，甚至他們何時暴露在此類事件的風險中。

參議院商業委員會主席Sen. John D. Rockefeller IV呼籲SEC必須採取行動。他說：這個新的指導準則將會改變一切。它會讓市場在評估企業時將其維持網路安全的能力納入考量。

SEC的指導準則係明確規定一項長期的要求，即企業需揭露重大事件的發展或投資人想知道的重大事件，且這個指導準則指出網路攻擊也不能例外。

舉例來說，一家公司可能需要揭露消費者資料外洩的重大入侵事件的成本和後果。這家公司的營收可能受損，而且也可能被迫花更多錢去加強網路安全或訴訟。另外，如果一家公司對於抵抗網路攻擊太過脆弱，投資人必須被告知這個風險。

專家說這個行動將企業安全的模糊地提升到較透明的方向邁向重要的一大步，而且也將喚醒企業對於保護網路安全的自覺。美國官員聲稱對抗來自中國及其他國家對於美國企業的駭客攻擊是國家及經濟安全的議題，而且瞭解這個問題涉及的層面才是有效回應此類問題的關鍵。

全球網路風險執行長Jody Westby說企業不太可能揭露這些突發事件。Westby說一家財富雜誌 100 大的企業在 2008 年遭受網路攻擊後，她曾建議他們將此回報給SEC。但是這個企業並不認同。遭受到網路攻擊的企業非常不願意揭露他們所發生的事，也很少回報給SEC。為什麼呢？因為害怕遭受商譽的損失。

專家說這就是為何指導準則有其必要性—強調揭露重大入侵事件的是企業的義務。

位於密西根州Traverse City的研究團隊Ponemon Institute主席Larry Ponemon說：揭露潛藏風險對於企業來說是沒有意義的，因為企業隨時都處於風險當中。而且幾乎所有重要組織都曾遭遇過網路攻擊。他預測企業仍然只會揭露極少部分。

前SEC官員現任Stroz Friedberg安全顧問John Reed Stark說：有些公司也許希望揭露駭客攻擊事件，但是他們並不知道如何評估其遭受到的損害。現在SEC已開始採取行動了，他並主張SEC應給予企業一些迴旋空間，否則可能會造成混亂。

Covington & Burling證券操作部門主管David B.H. Martin認為不揭露網路攻擊事件的企業可能會面臨許多不同的結果，例如：這些企業可能會被股東告或被SEC強制執行，而監管當局也可以發文要求他們改善其揭露情況。

計算網路竊盜的成本，無論是就打擊犯罪或是刺探間諜活動的目的而言，都是困難的。The Ponemon Institute發現每一次侵害的平均成本介於 500 萬美元至 800 萬美元間，但要評估受侵害的 50 家公司的影響需要耗時 9 個月的時間。

非營利組織 U.S. Cyber Consequences Unit經濟學家Scott Borg說：企業通常並不知道資料損失的價值或嚴重程度。利用美國經濟分析局的資料分析，他估計每年網路竊盜所產生的損失約 60 億美元至 200 億美元。（資料來源：The Washington Post，2011 年 10 月 15 日。）

摘自：國際公司治理發展簡訊第 49 期（2011 年 11 月 15 日出刊）