

名家觀點／落實資安治理 官民當務之急

2020-06-10 00:35 經濟日報 / 陳清祥

近日，國內多家重要的能源、科技公司，如中油、台塑、力成，在5月初接連遭到惡意網路攻擊。4月底衛福部疾管中心也曾傳出遭駭入侵，官員帳號外洩事件，520前夕總統府也驚傳遭駭。**近期資安事件頻傳，從民間企業到政府單位都受波及，網路攻擊已被視為全球最重大的安全威脅及風險，有賴檢調迅速調查釐清真相，更亟需儘快建立國家及企業資安防護機制。**

國內企業對於資訊安全的重視始終不足，直到2016年7月，一銀爆發大規模ATM遭駭盜領案，主管機關開始要求金融業辦理電腦系統資訊安全評估，2017年3月底更在金控及銀行內控內稽辦法中，增訂要求銀行業應設置資訊安全專責單位及主管，之後又擴及保險業。

金融機構因法規要求，紛紛開始重視資安，檢查局也將「資通安全管理」列入年度金融檢查重點。但是，非金融機構則常認為資訊安全是IT部門或資訊長的事。

終於，資通安全管理辦法及其子法在2019年上路，對於公務機關及特定非公務機關資通安全管理，要求依照資通安全責任等級分級辦法，配置資通安全長及增加資安專職人員配置等。特定非公務機關包括關鍵基礎設施提供者，公營事業及政府捐助的財團法人。上述中油及總統府資安事件，正是檢視該管理辦法是否落實的最佳時機。

為引導上市櫃公司朝最佳實務邁進，2019年公司治理評鑑，新增指標2.24「公司是否建置資訊安全風險管理架構，訂定資訊安全政策及具體管理方案，並揭露於公司網站或年報？」經過一連串駭客入侵事件後，上市櫃公司應更認真思考如何提升資安管理的層級，認真看待資訊安全風險管理。

法令只是最低要求，無論所屬行業為何，資安議題都很重要。不是為了公司治理評鑑得分，而是當駭客入侵時，重創的就不只是營運、財務面而已，甚至可能衝擊公司聲譽及客戶的信任。身為公司董監事，應立即關心一下公司的資訊安全管理。

首先，資安涉及科技、更涉及人員及文化，和公司營運及業務發展是息息相關的。人是資安控管最弱的一環，駭客經常運用社交工程手法，誘騙受害者進行違反規定的行為，要強化重視資安的文化必須由管理階層做起，除了要以身作則，並要透過各種場合及活動，持續灌輸同仁對資安的重視，並建立自我防護觀念，才能提升企業整體資訊安全的意識，降低資安風險。

其次，應確實評估什麼是公司最需要保護的「關鍵資產」，例如：智慧財產權（含營業祕密）等。還有那些資料或資訊系統對企業營收或重要業務流程影響最深，公司如何採取適當措施來保護及監控這些關鍵系統、資料或服務，針對常見的惡意攻擊，公司所採取的資安防護措施為何。

隨著新興科技及解決方案的日新月異，駭客攻擊手法愈趨複雜，資安風險管理也應與時俱進，針對各項風險建立適當的

資訊安全風險監控，與關鍵業務委外風險評估機制，確保各類資安風險均有效控制。

面對資安風險，除了建構事前防禦機制外，應強化事中的運作監控，更應建立事後應變處理機制，以降低資安事件可能產生的損失。建議公司董事會及審計委員會應加以高度重視，立即督導經營團隊建置及落實資訊安全風險管理，委託外部專業顧問和專責單位，共同研擬強化資安防護計畫，投入足夠資源，以確保資安策略的推動與落實。（作者是中華公司治理協會理事長）



訂閱udn兩岸財經報

訂閱

刊登廣告 | FAQ·客服 | 新聞授權 | 服務條款·著作權·隱私權聲明 | 聯合報系 | 訂報紙 | 關於我們 | 網站總覽

聯合線上公司 著作權所有 ©2020