如何解決資訊安全問題

趙真

目前台灣企業的資訊安全防護普遍並不足夠，缺少專職資訊安全人員是目前市場上普遍而且一致的看法，但是企業內部既有資訊人員對於資訊安全相關技術並不足夠才是一大隱憂，這點從另一方面來解釋，其實與管理高層缺乏資訊安全思維有關。在 2018 台灣駭客年會中亥客書院教學發展組組長張智凱曾表示過，在資訊安全領域中「看不到事情就表示有效」，但其實這與一般企業管理高層追求「看得到」的具體效益相違背，因此很難說服管理高層在資訊安全領域持續投入經費。

近年來，全球包含台灣的眾多企業飽受資訊安全威脅，DDoS 阻斷服務攻擊、Ransomware 勒索軟體、APT 進階持續性滲透攻擊…等事件頻傳，不斷持續延燒的各類資訊安全事件，不僅讓各企業面臨前所未有的威脅，也造成驚人的損失與傷害，尤其在干擾企業營運或工廠製造、損失機密或敏感性資料，甚至實體財產的損害上都有顯著的實例，另一方面，也許這對資訊安全管理來說反而是一個契機。

透過曾發生具有指標性的資訊安全攻擊事件，協助董事會與管理高層理解目前企業面臨的資訊安全防護處境，包含相關的教育訓練、資訊安全設備及工具上各種有不同程度的缺乏。主要是去正視資訊安全威脅並妥善地因應，並不是利用員工取得多少證照或通過多少考試就代表防護實力的增長，而是要在因應的層級上，從實務管理著手，去回應董事會與管理高層的期盼。實務上，資訊安全管理可以從幾個面向思考：

一、文化：資訊安全管理若被員工視為找麻煩，成功的機會就不高，所以首先要建立信任管理的文化，更進一步利用一些演練活動深化資訊安全的認知，活動可以包含內部威脅管理、宣導與教育訓練。

二、風險與關聯性：企業在追求創新與速度的同時，不能忽略風險的重要，需

要辨識事物於處理時所面臨的風險，進一步瞭解合作夥伴及廠商上下游之間的關係與風險，並進行管理。

三、事件通報與危機處理：除了建置即時偵測與通報機制，更重要的是訂定資訊安全事故發生時的危機處理與回應機制。

四、優先順序：科技不斷演進，駭客技術日新月異，資訊安全是永遠做不完的專案，可是企業資源不是無限的，必須依照管理的角度設定防護標的以及資源優先順序。

五、規範流程：制定企業安全政策與流程，降低人為問題發生率。

無論是科技上快速的創新，科技犯罪分子也將對利用漏洞的方式有全新的可能性，利用上述面向檢視，也許會得到一個人工智慧對決人工智慧的結果。

一般看到的企業資訊安全現象都是結果表徵，例如個人電腦被病毒攻擊、企業或個人資料被木馬偷走，雖然可以透過教育訓練與安全政策來解決資訊安全問題，不過人總是會有惰性，所以才需要靠規範與制度來約束。在解決資訊安全問題上，建議由上往下執行資訊安全防護，先進行各類型風險評估、定義作業安全規範、再建置所需安全設備與人力，才能有效的解決資訊安全問題，當然，對大部分的企業而言，這樣的方式會產生緩不濟急的現象，企業大多不可能等上幾個月甚至長達一年的評估時間，往往在現實環境中，大家還是以先解決問題再說。

資訊安全本身永遠沒有辦法被解決，只能把風險降低，所以企業本身應該先知道自己可以接受的資訊安全的風險底線在哪裡，所以才會需要由風險盤點開始，然而現實中都是碰上資訊安全問題後才去尋找解決方案，頭痛醫頭、腳痛醫腳的執行方式，缺乏對資訊安全的整體規畫，常常花費大量資訊安全投資後，仍無法有效解決問題，在缺乏完整的規畫下，無法發揮應有的功能，這才是首要應該解決的部份。

（圖檔取自網路）

本文作者：
和泰產物保險股份有限公司
資訊管理處協理