數位化經濟時代下新興科技的隱私安全風險與策略

基於全球化布局、行動化、互聯網、物聯網、雲端及大數據應用下，企業將面臨許多新穎科技所帶來之風險與衝擊，最近每每耳聞相關資安事件，且傳出災情的不乏國內外知名企業，如近期國內知名咖啡連鎖店傳出近 5 千筆客戶資料遭駭客入侵、美國政府人事局和內政部遭駭客入侵、日本國民年金機構近 125 萬筆國民個資外洩、美國國稅局超過 10 萬納稅人個人資料外洩等，再再顯示沒有百分之一百安全之事實，上述重大事件動輒影響民眾權益外，而且更影響企業長久來辛苦建立之聲譽。

根據 ITRC 資料外洩資料庫（ITRC Breach database）統計，2014 年全年共計發生 783 件身分資料外洩事件。身分資料外洩的資料筆數達 8,561 萬多筆，企業與政府單位因為罰金、訴訟費用或機密外洩造成龐大的金額損失。

因此近期美國白宮宣布成立網路情報整合中心，以解決日益嚴重的網路攻擊和隱私資料與商業機密的外洩問題，此中心主要扮演全國性的網路威脅情報中樞，將協調整合匯聯邦調查局（FBI）、中央情報局（CIA）及國家安全局（NSA）等多部門的情報力量，以提高美國防範和應對網路攻擊的能力。

依據勤業眾信與美國州際首席資訊長國家協會所進行 2014 年美國政府 CISO 資安治理調查報告內容顯示，目前雲端、行動與物聯網應用下威脅日增，如何於有限資安預算及資安策略未具體執行問題下，因應及展示資訊安全投資績效，並找到適切之資安人才，變成目前各企業皆需面臨之挑戰。

因此建議以下因應對策：

◆ 與業務溝通資安風險，以爭取預算

◆評估資安投資與管控有效性

◆ CISO 位階、職責強化與標準化

◆與人事單位協同培養專才

◆資訊安全委外策略運用

◆建立資安情資分析與因應機制

◆定期進行資訊安全健檢

從勤業眾信的觀點來看，金融業應採取事前蒐集監控、事中偵測應變及事後鑑識分析觀點，可依據所投入資訊安全資源，參照勤業眾信事前蒐集監控、事中偵測應變及事後鑑識分析之成熟度指標進行整體評估與建置。事前蒐集監控、事中偵測應變及事後鑑識分析之整體成熟度指標說明。

（一）事前偵測階段：

1. 日誌與威脅情報蒐集

建議企業需要由傳統被動式單點資安防護，轉為全面性積極主動防範，建立外部資安情報（Cyber Intelligence）蒐集與分析管理能力。

2. 日常監控

結合外部資安情報（CyberIntelligence）預警分析與管理能力，及逐步擴大內部稽核軌跡留存的種類，利用資料分析（Data Analysis）及異常行為規則建置（人、事、時、地、物之異常指標），得以回望過去（分析過往發生什麼事）、洞悉未來並提出預測（告警機制模型），以期設計異常行為之情境察覺系統，以風險計分模式為概念，任現風險儀表板，實現企業級風險管理機制。

（二）事中回應階段：

於事中回應階段，建議企業應透過通報程序與應變計畫建立，定期進行資安駭客攻防演練，以確保同仁皆有遵循的一致性作法及步驟、得迅速通報及進行緊急應變處置、提昇同仁資訊安全事件之應變回應能力及強化人員危機意識，相關重點應包含以下項目：

1. 建立應變組織

企業應明確定義相關權責單位，當事件發生時，人員能依其職務進行處理，並於適當時機召開處理討論會議，使會議決策能有效下達至各單位，進行危機應變處理。

2. 規劃事件應變處理流程

應依據事前規劃的事件等級，由相關人員進行通報與處理，並考量證據保全機制，另於事件結束後召開檢討會議，以記取相關教訓並徹底改善。

3. 規劃定期資安事件與駭客攻防

演練流程

平時應透過模擬真實攻防與演練方式，以駭客攻防與調查分析演練平台方式，培育理論與實作兼具的資安人才並提昇同仁資訊安全事件之應變回應能力。

（三）事後鑑識分析階段

企業於應變止血後，對於相關的情況進行細部調查而可能進入到訴訟階段時，應留存資訊安全事故之相關紀錄、日誌，該紀錄應妥善保存、確保完整、及最小更動，該紀錄應可被驗證，以確認其證據能力。良好規劃過的數位鑑識機制能有效協助企業在此部份的運作；以下就幾個面向，提供企業規劃數位鑑識管理機制參考：

1. 建置內部鑑識團隊

根據企業內部可能第一線接獲通報或發現事件之人員，教育其應變時，應小心處理過程可能對證據的影響。

2. 數位鑑識標準作業程序擬定

由於現在國內的標準程序尚未確認，因此建議參考數位鑑識相關國際最佳實務所提之作法進行整體規劃，如 ISO/IEC 27037 現場證據識別、蒐集、擷取與運送國際標準及 ISO/IEC 17025 國際實際室標準(數位鑑識項目)，使其能符合國內外要求，在國內數位鑑識相關程序尚未標準化前，對於法官將有很大的參考價值。

3. 數位鑑識蒐證及分析環境建置

此部份端看企業能負擔之其情況進行購置，但若礙於成本考量，其實坊間也有不少免費使用或價格低廉的鑑識分析工具可供參考，建議至少可購置第一線人員數位證據保全工具及硬碟鑑識複製設備。

4. 數位鑑識演練機制規劃

在人員訓練足夠、程序完整、工具齊備的情況下，最好透過不同情境的演練，以增加人員數位證據保全處理能力，以使相關流程運作能更加順暢及合乎法律原則。

結論

企業應建立事前主動蒐集與監控機制及足夠之應變措施準備，使人員知道事件發生時應如何進行初步判定與處理，通報適當主管與人員進行損害控制，有效與客戶或大眾溝通避免企業形象的受損,甚至由數位鑑識團隊進駐協助調查,並在事件調查至一定程度後，請教相關律師可能的訴訟議題，並擬定訴訟策略。如此，從事前防控、事中應變及事後處理等角度，以風險管理的思維完整規劃適合組織的作法，秉持「勿恃敵之不來，恃吾有以待之」精神,持續完善各該機關及所屬之資訊安全工作,並落實在日常各項作業中，才能使企業在現今充滿威脅的大環境下，仍能穩健地營運下去。

（作者為勤業眾信風險治理諮詢公司董事總經理-摘自法務部調查局清流月刊）