資料外洩代價知多少？

企管顧問公司勤業眾信（Deloitte）發現，資料外洩對企業造成的影響，「隱藏成本」可能高達九成，而且影響將延續到事情發生兩年或更久之後。

文／David Weldon 譯／葉庭筠

網路攻擊愈來愈頻繁，火力愈來愈猛，這點沒人會否認。而且大部份企業也都證實他們至少遭到一次網路攻擊。但這些企業真的了解資安攻擊的影響全貌嗎？其實，和資料外洩相關的直接成本遠比「隱藏成本」來得輕微。

所謂「隱藏成本」可能高達企業總體損失的九成，而且影響將延續到事情發生兩年或更久之後。這些是企管顧問公司勤業眾信（Deloitte & Touche LLP）最近發表名為《網路攻擊的表面下：深入探討企業影響》（Beneath the Surface of a Cyberattack: A Deeper Look at the Business Impacts）的研究發現之一。

勤業眾信列出了網路攻擊的14種企業影響，這又可分成「表面上」或為人熟知的事件成本，以及「表面下」或不易見或隱藏成本兩大類，每大類各7 種。

但勤業眾信相信現行對網路攻擊市值的估算遭大幅低估，因為大眾只注意到「表面上」的成本，但這只佔很小的比例。

「企業主管往往難以判定可能的損失，原因之一是他們不知道同業為了恢復正常營運吃了多少苦頭，」勤業眾信首席分析師暨顧問網路攻擊因應方案主管Emily Mossburg 指出，「網路攻擊影響一直缺乏精確評估，使企業也無法建立必要的風險準備。」

「許多討論重點都還在漏洞長得樣、科技影響為何的層面上，大家只關心外洩時的通知以及事後還補足什麼防護機制，似乎沒人關心更廣泛的影響。」

勤業眾信分析師於是決定一探網路攻擊的影響全貌。

「我們原本只知道這部份是被低估了，但我們並不確定有多少比例被隱藏在表面下，而為現今網路攻擊討論所忽略，」Mossburg解釋。

為了說明網路攻擊的影響，勤業眾信研究團隊列出了二個虛構企業案例，並假設五年間各種損失金額。資料外洩造成企業的影響或成本可分成以下14類：

表面上或已知的網路事件成本：

- 客戶外洩通知
- 外洩後的客戶防護
- 法規遵循（罰款）
- 公關／危機溝通
- 律師費與官司費用
- 網路安全的改善
- 技術調查

表面下或隱藏、不明顯的成本：

- 保險費增加
- 舉債成本增加
- 營運中斷
- 客戶關係價值損失
- 品牌價值降低
- 智財（IP）損失

上述14類成本中，最嚴重的要算是營運中斷的損失。

「每家公司的影響樣貌都不一樣，但各產業在某些重要領域是共

通的。例如，零售業信手卡資料最重要，健康照護業則是可辨識個人資訊（personally identifiable information, PIN）。在製造業，智財損失影響最大。但是對所有公司來說最常被低估的影響是業務中斷，」EMT Consulting 首席顧問暨總裁，也是SIM網路安全集團成員Erik Thomas 表示。

「視時間點和事件期間而定，可能衍生出罰金、營收損失、借貸成本、客戶服務、品牌價值和未來商機等廣泛影響，」Thomas說。

愛達荷國家實驗室的資訊長Darren Van Booven 也認同。他說，「最明顯、最容易感受到的影響，是事件引發的經濟面成本，要擋得住和回應攻擊、調查後續的資料外洩、公關災難、主管機關罰款、信用盜刷監控服務，以及強化後端防禦以免重蹈覆轍等等。對不論小型或大型企業來說，可能隨便就要幾百萬美元。」

此外還有看不見的成本，Van Booven指「視企業規模、事件屬性，以及所處規模等多種因素而定，影響可能包括喪失有效資訊保護的能力，而這引發的企業客戶反應又因產業不同，金融業就會比大宗製造業來得大。」

「這些成本較難估計，但如果投資人、客戶或重要合作夥伴反彈強烈的話，集結起來後果不可小覷，」Van Booven解釋。

RSA技術長 Zulfikar Ramzan 列出網路攻擊的五大影響包括：商業永續性受影響、智財被竊、敏感資料如客戶及員工資訊外流、法規遵循影響（被罰）及名譽損失等。

「依據各企業及垂直產業的差異，大家的排序一定也不儘相同，有的領域如商業永續性比較好量化，但有的領域就很難給個數字，例如智財損失。」

影響的成本

但勤業眾信分析師還是想把它算出來。報告裏模擬兩家遭到網路攻擊的企業，來說明可能發生的14類損失。

例子一是一家健康照護公司，該公司一台含有280萬筆客戶個人健康資訊（personal health information, PHI）的筆電在其健康照護分析軟體廠商處被竊，造成資料外洩。按照14種影響因子計算，該公司資料外洩損失總計16.79億美元，細分如下：

- 客戶外洩通知：6個月，1000萬（佔總成本的0.6%）
- 外洩後客戶資訊保護：3年，2100萬（1.25%）
- 法規遵循：兩年期間共200萬（0.12%）
- 公關／危機溝通：第一年100萬（0.06%）
- 律師費及官司費用：5年1000萬（0.6%）
- 網路安全改善：第一年1400萬（0.83%）
- 技術調查：6星期100萬（0.06%）

表面下成本：

- 保險費成本增加：3年4000萬（2.38%）
- 舉債成本增加：6000萬（3.57%）
- 營運中斷：3000萬（1.79%）
- 客戶關係價值損失：3年4.3億（25.61%）
- 合約營收損失：3年8.3億（49.43%）
- 品牌價值減損：5年2.3億（13.7%）
- 智財損失：無

那麼，企業該怎麼防止這些損失發生呢？Mossberg建議從以下四個面向著手：

「總結看來，我們從四個不同面向來評估企業該如何改進：第一、也是最重要的是計畫元素：包括策略、治理、政策、程序、框架，這些方面在公司整體計畫下是否有不足而需要補強的？」

「第二是企業的主動安全控制和準備，即他們是否有做好措施來保護其資料、系統、環境，以及最重要的，他們的業務。」

「第三是他們是不是有持續了解及監控環境動態的措施。例如他們是否有工具可紀錄系統上的活動，是否有工具可分析異常活動？」

「最後一項是，企業是否隨時準備好回應安全事件？靈活性夠不夠？他們是否有回應事件的流程？這些流程和計畫是否經過測試？從基層到高層人員，企業知不知道事情發生時該聯繫誰？」