電商平台坦誠兩年前遭駭客入侵，至少五億用戶帳號被竊

【焦點話題】

2016 年 8 月某電商網站傳出曾有 2 億用戶資料被盜，並流入黑市販售。美國媒體 Recode 報導實際外洩情形更為嚴重，某電商網站隨後於證實該公司於 2014 年遭駭入，至少 5 億美國用戶姓名、電子郵件信箱、電話、加密後的密碼及生日遭到竊取，另部份用戶的安全問題與答案亦有外流，但遭竊資料未涵蓋銀行帳號或信用卡資訊等。某電商網站表示已取消部分用戶以答覆安全問題登入的方式，並積極配合執法單位進行調查，該公司相信這樁駭客行動背後有國家力量的支持，同時呼籲 2014 年以後未變更密碼的用戶儘速更改密碼。【資料來源：iThome，105/9/23】

【重點摘要】

1. 電商網站維護會員資料庫安全性，得採取的技術上措施可能包含主機架設防火牆、建立異常偵測機制或定期進行弱點掃描等。
2. 因應電商網站個資外洩規模與頻率迅速攀升，我國已由主管機關積極透過個資法上行政檢查措施，並配合相關改善輔導機制，督促業者落實相關義務，以從資訊安全角度根本降低外洩風險。

【法律觀點】

依我國個人資料保護法（簡稱個資法）規定，公務機關或非公務機關發生個資事故後，應查明後以適當方式通知當事人，通知內容應包含個人資料被侵害之事實，以及已採取之因應措施。本案例中該電商網站雖為外國公司，但事故發生後，亦取消部分用戶安全問答登入機制，且呼籲用戶更改密碼作為補救措施，以減少損害擴大。又，本案例之事件並非單一個案，隨著近來電商網站個資外洩規模

迅速攀升，資訊安全議題更加引發社會大眾重視。企業依個資法須採取組織上與技術上適當安全維護措施，以妥善維護個資安全。對於電商網站維護會員資料庫安全性，得採取的技術上措施可能包含主機架設防火牆、建立異常偵測機制或定期進行弱點掃描等。本次事件中，某電商網站並非自行發現遭到駭客入侵，而是個資外洩長達兩年且傳出黑市交易傳聞後，啟動內部調查才證實確實發生個資事故，此亦突顯出駭客手法趨於隱蔽，致企業難以察覺或防範。

考量到個資外洩導致網路詐騙猖獗，進而造成民眾財產損失，經濟部商業司為促使業者正視問題並加強改進，已於 2015 年 4 月邀集相關部會與專家，共同組成「網際網路零售商品之公司行號個資保護行政檢查小組」，將發生重大個資外洩或突發性嚴重個資外洩業者列為行政檢查對象，依個資法辦理行政檢查，以強化對於網路零售平台個資保護情形之監督，若業者經通知改善後仍未改善，則主管機關可按次依個資法處新臺幣（下同）2 萬至 20 萬元罰鍰。故我國針對此類電子商務網站，已由主管機關積極透過行政檢查並配合相關輔導措施，督促業者落實相關義務，以從資訊安全角度根本降低外洩風險。

【管理 Tips】

首先，組織是持續曝露在資訊安全風險的環境威脅下運作的。公司應當定期識別出相關技術脆弱性，並建立與支援脆弱性管理所需之資訊，包含脆弱性監視、風險評鑑、修補程式、資產追蹤及所有必要之協調責任，以降低組織受到的資訊安全風險的威脅。應定期審查組織內資訊系統的脆弱性威脅，包含運用滲透測試、弱點掃描及人工檢查等方式，檢驗運作之系統的安全性，並隨時關注新技術、新型病毒及駭客模式，以隨時更新資訊安全知識，讓組織保持受防護的狀態。

再者，組織在面對資訊安全事故時，需建立起管理責任及程序，以確保對事故的發生可以迅速、有效及有序的回應。為此，需規劃適當的通報管道、記錄事件發生的狀態及原因、對事故發生時的緊急回應以及從資訊安全事件中組織的成長與學習等等。以上皆為面對事故發生時的應變措施，這些程序都需事先做規劃，並定期的做演練，以避免實際發生時帶來負面的影響。

資料來源：

行政院國家資通安全會報技術服務中心法律彙編