【解牛集】

資訊安全靠一方保護損害更大

許佳龍
科大資訊、商業統計及營運管理學系講座教授

就近日三宗個人資料外洩的網絡保安事故，包括國泰航空公司九百多萬名乘客的資料遭不當取覽、英航客戶的信用卡資料外洩，以及轉數快所出現的安檢驗証紕漏，筆者上周撰文指出，若當事企業聘用第三方服務供應商的資訊保安出現問題，則這個「第三方」風險便很可能給黑客打開入侵之門，從而殃及當事企業或機構的網絡系統遭受淪陷，故企業對此「第三方」風險不能掉以輕心。

當下，個人的生活已離不開資訊網絡，而個人資料外洩事件又層出不窮，更關鍵一點是，隨著資訊科技不斷創新和網絡活動更為普及化，很多個人資料外洩的紕漏源頭和網絡犯罪，往往又以「嶄新」的來源和形式出現，令人防不勝防，因此，如何提高個人和企業對資訊保安的意識，是配合資訊社會發展不可或缺的環節，尤其企業因客戶資料外洩而引起的法律訴訟賠償風險，如何做到事前防備、事發因應、事後補救這「三步曲」，必須認真思考；另一方面，在應對個人資料外洩和網絡商業犯罪事故有增無減情況下，政府如何制訂網絡安全標準，同樣是一個非常值得討論的迫切議題。

事前防範避免掛一漏萬

今次國泰航空乘客資料外洩事件，國泰在事前防備上——若報導屬實，即該公司外判網絡安全供應商進行「入侵測試」，以檢測自身的系統有沒有安全紕漏，但外判網絡安全服務商不小心以國泰航空客戶真實資料作系統測試，其後遭黑客入侵，以致國泰約 940 萬名乘客的資料遭不當取覽。很顯然，在事前預防上，國泰有忽略「第三方」風險之嫌，在防備上有所缺失。

記得筆者曾探討劍橋分析公司（CambridgeAnalytica）利用臉書（Facebook）平台上的漏洞，未經許可收集了逾 5000 萬臉書用戶的信息資料。事故中，個人資料外洩的規模龐大，殃及的人數眾多，以千萬單位計，關鍵之處，是負責收集資料的劍橋心理學教授科根（AleksandrKogan），透過一個性格測試的 APP，邀請臉書的用戶參與測試，科根則收集登錄臉書帳號參與者的個人資訊與點贊記錄。除受訪者本人外，再通過收集受訪者在臉書上的好友資料。當時，參與性格測試的人數約 32 萬人，但科根順勝摸瓜，加上用戶在臉書上的好友，像滾雪球般，讓他輕易收集到逾 5000 萬臉書使用者的資料——這個「友朋間信息披露」（Peer-Disclosure）風險的網絡新現象，展示了個人對於保護自身的私人資料，同

樣帶有忽略「第三方」風險的意味。

可以說，在網絡系統相互勾連、多方向傳輸的今日網絡世界上，「第三方」風險，其「隱蔽性」往往受到忽略，卻又往往帶來防不勝防的巨大破壞性，因而無論是企業或個人，都必須對「第三方」風險提高警惕。

事後回應須早披露

回到國泰航空客戶資料外洩的事故，在防備上出現了漏洞，事發後，國泰因應事故的處理，亦有值得討論之處。由於事發於今年 3 月，但國泰航空到 10 月下旬，相隔逾半年才公開事件，無論當事機構如何解釋，其理由都難以令人信服。

很明顯，由事發到公開披露消息，時間相差了逾七個月，當中，容許黑客有很大「上下其手」作出攻擊的空間。為什麼國泰拖延公布而不盡快向外披露，使遭受資料外洩的受害客戶能夠盡快作出措施，去避免可能出現的損失，如及時通知相關銀行暫時停用信用卡、甚至馬上更改信用卡密碼，或電郵地址的登入密碼等，把握到避免或減少損失的黃金時機。

歐盟於今年 5 月下旬所落實的《通用數據保護條例》（（General Data Protection Regulation，GDPR），規定個人數據處理者必須清楚地披露任何數據收集，聲明數據處理的合法基礎和目的、保留數據的時間。如果數據洩露對用戶私隱產生不利影響，企業必須在 72 小時內向主管監督機構報告。盡快向外作信息披露的考量，是讓受影響的客戶能夠盡快作出應對，減少損失。

客戶失去自救黃金機會

事實上，企業遭黑客入侵，導致客戶個人資料外洩，若「秘而不宣」，不僅使客戶的利益受到更大的潛在損害，而且亦使公司事後面對更大的潛在訴訟風險。誠然，目前大部分企業對於公司遭黑客入侵，更傾向把事故「掩飾」，擔心公司聲譽受損，影響業務，且往往在事發之初，以免引起公眾無謂恐慌為由，公司需要時間去了解事故，甚至找出事故的確實原因，故而沒有及早向外公布。

然而，這種講法值得究詰，正如筆者上周的拙文所指出，網絡資訊系統的保安，需要涉及其中的各持份者共同維護、共同作出貢獻、共同承擔，而非單獨一方機構可以隻手解決，從這個角度看，國泰今次事故，客戶個人資料的安全和保安，並非完全是國泰一方的工作責任，客戶其實亦可以採取行動去保護自己。若出事公司能夠及早通知客戶其網絡系統出了問題，客戶便可以第一時間，去堵截個人資料外洩所出現的漏洞，包括及時刪去一些敏感資料、更改密碼，以至取消這個

戶口，做法多種多樣。反之，出事企業延宕通知客戶，獨力承擔保安的工作責任和「救火」，不僅令客戶失去協助公司堵截保安漏洞和事後及早作出補救措施的機會，亦使企業的損失更大。

事實上，企業應該明白，資訊的保安工作，公司無法獨力維護與承擔，因為保安系統是一個由牽涉其中各持份者共同作出貢獻和努力的共同成果，這一點十分重要。若企業對網絡入侵「秘而不宣」，害怕事故影響企業營運，只獨力去承擔和解決，最終會失去客戶的助力，大家共同去堵截漏洞，減少各自損失的機會。

安全標準「不安全」

隨著網絡犯罪和個人資料外洩事故不斷發生，網絡保安標準也愈來愈受到重視。筆者記得，無論是今年英國航空訂票系統遭黑客入侵，導致大批客戶信用卡資料外洩，抑或 2013 年 12 月底，美國僅次於 Walmart 的第二大連鎖商店 Target 遭到黑客入侵， Target 當時估計，約有 4000 萬名客戶的信用卡或簽帳卡資料被竊，這些公司其實都有參與一個業界稱為 PCIDSS 的信用卡付款保安標準（PCIDSS 是「支付卡產業安全標準協會」(Payment Card Industry Security Standard Council，PCISSC)為了保護持卡人資料及交易安全所訂定的標準，要求所有與支付卡處理相關聯的機構，包括商家、服務供應商、收單機構(Acquirer)及發卡機構(Issuer)都必須符合該標準。

這些參與 PCIDSS 的公司都聲稱有做足安全標準的要求，而顧客和政府亦相信公司有跟從了這個標準，但最後出現了問題，才發覺還有些地方沒有完全跟足。筆者一篇研究論文便深入分析了相關問題(有興趣的讀者可參看 Information Security Outsourcing withSystem Interdependency and MandatorySecurity Requirement,刊《Journal of Management Information Systems》 ， Winter 2012 – 13, Vol. 29, No. 3, pp. 117 – 155)。

安全標準愈高效果愈少

筆者的研究發現，為了滿足政府的網絡安全標準，業界定了安全標準後，很多公司外包給網絡安全供應商（managed security service provider，MSSP）去協助設立保安措施以迎合這些安全標準。論文深入分析發現，強制性的安全要求，使 MSSP 的生意愈來愈興隆，而且更不斷激勵它們為更多客戶提供服務，雖則有更多客戶可以得到 MSSP 的保護，但也導致隱含更多系統相互依賴風險。如果強制性要求很高，反而有機會提高來自第三方的網絡安全風險。

換句話說，強制性執行高安全標準，有機會加劇公司網絡保安上的損失。由此來

看，強制性安全標準的成果其實並不理想。主要原因是，企業除了外包給 MSSP 設立這個安全標準外，公司內部的資訊保安水平並沒有真正提高，中間還是有不少紕漏，成為黑客入侵的方便之門。事實上，安全標準愈高，除了給網絡安全服務供應商帶來更多生意外，全面性的安全保護利益未必提高，因而強制性安全高標準的政策並不可取。

與此同時，當所有公司都使用同一安全標準時，會導致系統之間的相互依賴風險，黑客只要成功攻擊一個系統，其他公司的網絡系統安全也可以遭攻陷。很顯然，當大家同一時間接受了這個安全標準，卻又沒有做好自身內部系統的安全，所冒黑客入侵的風險反而更大。

總體來說，個人資料的保護，企業如何做到事前防備、事發因應、事後補救當然很重要，但資訊安全的效率得以提高，必須建立在牽涉其中各持份者共同努力和貢獻的基礎上，企業獨力維護孤掌難鳴，大家也要明白「第三方」的存在和隱性破壞力，這無疑是近日多宗個人資料外洩所給予我們的啟迪和教誨。

〔本文由科大商學院傳訊部筆錄，許佳龍教授口述及整理定稿，文章在信報 11 月 12 日發表〕