【解牛集】— 刊於《信報》，2019 年 8 月 26 日

保密訊息外洩「內鬼陷阱」

許佳龍

科大資訊、商業統計及營運管理學系講座教授

美國第五大信用卡發行商 Capital One Financial Corp.上月底遭「黑客」入侵，盜取了該公司存儲在亞馬遜網絡服務（AWS）的雲計算服務上約 1.06 億信用卡客戶和申請人的個人信息數據，成為年來一宗令人觸目的網絡保安事故。

這名後來被捕的涉嫌「黑客」，竟然是 AWS 的雲計算服務部門前僱員佩齊·湯普森（Paige A. Thompson），擔任系統工程師。在 AWS 工作期間，她能夠訪問存儲在雲計算服務上的數據。據初步調查，湯姆森發現 Capital One 系統的一個入口缺漏，並利用某些配置錯誤的網絡弱點鑽了空子，輕易把大規模數據予取予攜。很顯然，作為該公司的系統工程師，湯姆森對 AWS 雲計算服務的系統應有所了解，這宗數據外洩事件，再次突顯了一個網絡保安弱點——「內鬼」難防。

「防火牆」難防內鬼

事實上，對擁有大量客戶資料的機構，一旦進行了網絡數據處理，都會建構一道「防火牆」，以防範外來「黑客」的網絡入侵，盜取數據。公司的防範重點，一般都著眼於外部，甚至在設定系統或網絡時，傾向認為外人不可信，但內部人員可信，以致把重點在嚴防來自外部的網絡風險，因而如何防範來自內部可能導致數據外洩的風險因素，往往受到忽略。但偏偏這個被忽略的部分絕對不宜掉以輕心。我們看到，由內部導致數據外洩或數據處理失當對公司所造成的損傷，往往有「致命性」後果。

記得去年爆發的「劍橋分析公司（Cambridge Analytica）事件」，該公司員工威利（Christopher Wylie）去年 3 月下旬，自稱因為良心不安，打破了離職保密協定，向英國的衛報（The Guardian）揭露 Cambridge Analytica 如何非法取得臉書 5000 萬個用戶資料，並分析這些數據資料後，掌握了龐大用戶群的行為和價值偏好，於是在 2016 美國總統大選期間，針對這些用戶選民的偏好，在各社群媒體投放各式「假新聞」和個人化宣傳廣告，以影響中間選民的投票行為。事件揭露後，劍橋分析公司當然成為眾矢之的，最終也擺脫不了走上倒閉的厄運。

可以看到，在網絡世界，多宗大規模個人資料外洩和數據處理失當導致公司損失慘重的個案，很多都是來自內部的風險因素。

須設立適當使用權限

應對內部員工的洩露信息資料或數據處理失當行為，機構可以通過設立使用權限來加以制約。然而，一些企業對此並不積極，因為此舉會增加系統設計的成本，而且這樣做，難免需要對機構內部所有員工作出「分層」，造成「有權限者」和「無權限者」之間的相互信任問題，有機會損害到公司上下一心的整體工作團結性，甚至不排除引起公司出現一些「辦公室政治」。

事實上，不少銀行的客戶私隱資料外洩造成的「災難性」事故，往往是內部員工的「傑作」。

討論至此，不妨看看 1995 年爆發的英國霸菱銀行（Barings Bank）倒閉事件。該行在新加坡設立分行，計劃大展拳腳，並派遣當時年僅 26 歲的交易員李森（Nick Leeson）到新加坡分行，擔任期貨部門任首席交易員，專責期貨與期權的交易。

李森可能急於表現自己的工作能力，從事了一些未得銀行授權的交易，並從 1992 年便開始隱瞞投資虧損。由於李森熟悉電腦，他投資成功獲利所得，便記在霸菱銀行的投資交易專項帳戶中，讓該行高層對他的投資成果一目了然，得到該行「投資明星」之譽；但對於投資失利的損失，他則轉記到一個試驗帳戶

（Test Account） 中——一個模擬投資的帳戶裡，起初的確「神不知、鬼不覺」。

霸菱銀行倒閉之路

1994 年底，李森預測日本的股票價格與利率水平可望因經濟復蘇而回升，於是在新加坡及日本期貨交易所大舉買入日經 225 指數期貨，並沽空日本債券期貨。誰知「人算不如天算」。1995 年 1 月 17 日，日本發生阪神大地震，重創日本經濟，連累日本股市大跌，使李森的交易飽受重創，損失逾 2 億美元。他試圖力挽狂瀾，一方面竄改交易紀錄，向霸菱銀行掩飾虧損；另一方面進行風險更高的投資交易，並採取空頭跨部位（short straddle）的期權投資策略，投資細節不必細表，但結果虧損的泥潭反而進一步深陷，最後，銀行發現李森的交易累積的損失高達 14 億美元，是銀行資本額的兩倍，出現資不抵債，導致銀行倒閉。最後，以 1 英鎊的象徵價格，賣給荷蘭 ING 集團。

對於霸菱銀行倒閉事件，很多分析認為此事屬於未獲銀行授權的「不合法」交易。但嚴格來說，其實是一起資訊保安事件。由於銀行當時設計的電腦系統，容許李森能夠同時取用多個帳戶，讓他隨時把虧損在帳戶間進行「挪移」，這種缺乏權限使用的系統設計，最終造成無窮遺恨。

無心之失與有心之害

這類資訊系統或網絡保安的「內鬼」問題，如何防範，的確令人費煞思量。筆者接觸過的案例，亦曾發現有機構員工，盜取了公司的機密資料，售賣給公司的競爭對手。這些「內鬼」網絡保安風險，企業有必要加以注視，做法包括檢視電腦或網絡系統可能出現的「內鬼」風險，設立適當權限使用的制度。

特別指出，機構與員工之間在進行網絡保安或信息保護上的「誘因」（incentive）往往不一致。公司的目的，著眼盈利之餘，還會考量和防範對公司傷害的風險。在風險問題上，公司承受的風險遠高於員工，兩者顯然不成比例。因此，公司高層必須明白，從員工的角度看，他們不一定有強烈的誘因，去減低網絡保安風險或力保客戶資料不外洩。

當然，員工在「有心」或「無心」的情況下，釀成「內鬼」事故。若員工為無心之失，或可透過「教育」，使員工明白正確處理數據的方法和程序。若員工「有心」去「出賣」公司的利益，則公司必須明白「有心人」何以作出破壞公司網絡保安或惡意洩露公司客戶資料的可能性，例如，出於憎恨？——也許員工覺得所得薪酬偏低、公司對他不公平、受到無理責罵等.....出於報復之心。

另一方面，有時候，員工也非出於報復心，而是想在工作上 「走捷徑」，讓自己的工作快一點、或輕鬆一點完成，盡快放下工作責任，因而做出公司所不容許的「不合法」的網絡內部入侵行為。

合規工作行為賞罰制度

事實上，有心去損害公司網絡保安或洩露公司保密訊息的員工，動機多種多樣，如員工與上司不和，都有成為「內鬼」的犯事的動機。因此，對於來自內部的保安風險，公司需要訂出清晰的工作程序和誘因，去讓員工遵守，立足於工作正軌，並設立賞罰制度，強化員工合規工作的積極性。

誠然，員工跟公司有齟齬，原因的確多種多樣，可以是出於跟同事和上司相處不和而引起，也可以純粹是員工的職業道德出了問題，對挪用公司資源毫無悔吝之心，甚至認為是合理行為，因此，每一家公司，因應不同的國家文化、公司文化以至當地群體行為的道德價值，採取相應措施，從制度上去防範「內鬼」風險，大方向包括一、設立適當的使用權限制度；二、設立工作合規性的賞罰制度。

教育與自律不可或缺

總的來說，在今日網絡世界，由於資訊科技發展日新月異，因而存在不少業務經營的「灰色」地帶，因而，合規經營和工作，不僅公司的員工需要自律，公司的營運也需要遵守和實踐。在美國，一些「內鬼」事件，員工之所以自甘成

為「內鬼」，去揭露公司的秘密信息，不合規運作，如震驚國際的斯諾登（Edward Snowden）事件。這位前美國中央情報局職員，美國國家安全局外包技術員，在 2013 年 6 月將美國國家安全局關於稜鏡計劃監聽專案的秘密文件，披露給英國《衛報》和美國《華盛頓郵報》，迄今尚遭到美國和英國通緝。去年的「劍橋分析公司事件」，都牽涉到廣義的網絡合規性行為本質。員工「看不過眼」所屬機構的不合規經營行為作出「反噬」一口。

從資訊保安的角度看，「斯諾登事件」或「劍橋分析公司事件」，都是出於「內鬼」的事故，只不過這兩起「內鬼」行為是以「正義」的價值去支撐。因此，關於網絡保安的「內鬼」風險，公司除了確立適當的使用權限和員工合規工作行為的賞罰制度外，教育和自律無疑也是網絡保安不可或缺的支持要素。