【解牛集】— 刊於〈信報〉，2018 年 11 月 5 日

「第三方」風險予黑客可乘之機

許佳龍
科大資訊、商業統計及營運管理學系講座教授

近日，資訊保安出了三宗備受矚目的個人資料洩漏事故。第一宗，是國泰航空公司遭黑客入侵其系統，約 940 萬名乘客的資料外洩，包括個人名字、身分證號碼、地址、電話、信用卡號碼等被不當取覽。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，事故引起各界譁然。

第二宗是英國航空公司的訂票網站上月遭黑客入侵，24.4 萬名透過信用卡付款的客戶個人資料外洩，包括姓名、地址、信用卡號碼、有效期限及安全碼等資料。到 10 月 25 日，英航再向外披露，承認較早前遭黑客入侵盜取資料事故中，再有 18.5 萬名客戶資料懷疑在入侵中外洩。

轉數快現多宗轉帳騙案

第三宗涉及於 9 月底才開通的快速支付系統「轉數快」服務。參與這項新服務的銀行和儲值支付工具（電子錢包）營運商共 31 家，大家攜手提供實時跨銀行及電子錢包轉帳服務。不過，系統推出不足一個月，即有市民身份證及銀行戶口號碼被盜用，其賬戶在未經本人授權下，遭不法之徒透過「轉數快」增值到自己的電子錢包中。

從媒體的報導中可知，利用「轉數快」犯案的騙徒，首先騙取他人的身份證和銀行戶口號碼，然後到儲值支付工具營運商，用騙取得來的身份證開設一個儲值支付工具戶口，同時申請設立電子直接扣賬授權服務（eDDA）。之後便透過「轉數快」，向銀行發出直接扣帳授權服務要求，把受害人銀行戶口的錢，轉到冒他人之名開設的支付工具戶口中，再把電子錢包內的錢「搬走」。

「轉數快」開通短短半個月已有多人受害。其中一個受害人銀行帳戶內的 9.7 萬元存款，遭轉帳至支付寶帳戶，懷疑有人利用安檢認証上的漏洞，將受害人戶口內的錢，以增值方式轉至用她名義開設的支付寶戶口中。不法之徒共分 18 次將款項轉走，過程中，受害人毫不知情，事後收到銀行賬單，才得悉事件。

電子錢包開戶「兒戲」

據金管局所得的資料，事件中，約有十多個銀行帳號懷疑被盜，用以在電子錢包內開設 eDDA，除個別戶口金額逾萬元外，大多涉及數千元，總數約 18 萬元，數額不算龐大，但卻折射出資訊保安上一些很值得討論的問題。

嚴格來說，「轉數快」系統在轉賬服務上並無問題，關鍵在於支付工具服務商為何只需客人提供一個身份證的影象，便可以讓人「替他人」開立帳戶。這裡就引伸出一個電子系統保安上、也是企業與個人同樣值得警剔的安全概念——系統的相互依賴性（System Interdependency）。

很顯然，大家向顧客提供一項服務——例如「轉數快」，其實內裡牽涉其他一些不同的公司、不同的客戶，大家集體參與，並在項目服務的系統中，加入各自的安全努力與貢獻，最終系統才能安全地運作。換言之，資訊網絡的保安，是集體性的結集。

系統保安的相互依賴性

目前，大部分企業著眼其資訊系統時，只聚焦於自身的系統設計是否安全、措施是否足夠、在流程上有沒有保障或紕漏等，而忽略了一個最重要的環節——即系統的安全性，最終取決於系統內整體生態環境中各持份者所付出的努力。換句話說，資訊保安的有效性是建基於集體的努力，彼此相互勾連、相互依賴。

以國泰航空的洩漏事件為例。洩漏的原因，據報導是該公司請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，然而，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。誠然，在進行測試時，客戶——即國泰航空往往准許網絡安全服務商進入到自身系統中一些較為機密的區域或環境，若沒有仔細考量到服務供應商有沒有做足安全防護措施，或服務供應商這一方的資訊保安出現漏洞，便無可避免令自身的系統暴露在風險環境之中。

國泰航空客戶資料外洩的漏洞，若據聞屬實，則出事的關鍵似乎在於此。這一點，恰恰說明了筆者前文提到的資訊保安的系統「相互依賴」特性。事實上，明白系統的相互依賴性，對有效提升資訊保安相當重要。

外方風險防不勝防

其實，國泰航空自身的系統可能很安全，但當它擬增加一些額外服務，或額外的系統測試時，外部或外判服務供應商提供服務時，從外進內的可能潛在安全風險，有可能使自身系統受到感染，一旦這個環節出現保安漏洞，自身系統便可能受到殃及，予黑客可乘之機。

至於英航客戶的信用卡資料外洩，網上有不少分析，試圖去破解出事的關鍵。有未經証實的報導披露，個人信用卡資料外洩，或非出於英航的訂票系統遭黑客入侵，而可能在於所採用的其他網站收取信用卡款項時——一般使用第三方服務供應商，去進行支付結算或授權，在通常的情況下，網站設計所用的 Java Script，往往也是由第三方服務商供應。因此，英航的客戶資料外洩，大家懷疑，並非英航的客戶系統出現問題，而在於收取信用卡的服務供應商，其網頁有安全紕漏，以致在讀取信用卡付帳的過程中，已為黑客截取到信用卡持有人的個人資料，說法未嘗沒有根據。

換言之，服務供應商的安全風險，由外而內，帶進自身的系統之中。因此，客戶無論如何細心維護自身資訊系統的安全性，一旦使用第三方的服務，就會面對「防不勝防」的潛在安全風險威脅。

「第三方」風險是禍源

再看「轉數快」出事的問題。前文中已提及，付款方銀行的系統其實沒有問題，因銀行依照金管局的指示行事；客戶本身的銀行系統亦沒有問題，因為也沒有人入侵其系統盜取了客戶的資料，出事的關鍵，在於支付工具（電子錢包）供應商替客人設立戶口的程序，由於供應商沒有認証到客戶本人，只憑一張個人身份証就開立了戶口，開戶後，透過「轉數快」，便使不同銀行之間連成了一線。

由於「轉數快」以電子直接付款授權服務（eDDA）從銀行戶口轉賬至電子錢包，若果銀行或電子錢包供應商在進行電子直接付款授權服務時，雙雙都沒有向銀行戶主取得授權認證這個步驟，這樣一來，不法之徒只需取得別人的香港身份証和銀行帳號，便可以從受害人的銀行戶口，經「轉數快」以自動支付，轉走存款到「太空卡」登記的電子錢包，然後飽食遠颺。

無可諱言，銀行按照電子直接付款授權服務，把客戶帳號的錢轉至電子錢包增值，而沒有向銀行戶口戶主取得授權認証，當然有所缺失，但歸根究柢，儲值支付工具供應商最初在替客人開立戶口時，沒有向申請人進行認証，只憑一張身份証影象，就輕易開立帳戶，此舉無異是把安全風險，感染到轉帳付款方銀行的身上。

相互依賴性帶來額外風險

上述三個資訊安全出事例子清楚揭示，在資訊保安上，系統的相互依賴性，往往為系統本身帶來額外的安全風險。然而，目前大部分企業，在系統保安上，通常只聚焦於本身系統的安全性，如安全措施是否足夠，網絡系統是否存在漏洞，集中圍繞公司自身業務範疇所提供的服務系統，而忽略了「從外進內」的第三方服

務供應商、也可能是顧客，甚至是其業務或交易伙伴所帶來的安全風險與威脅。

目前，網絡系統接駁所有電腦可謂無遠弗屆，系統與系統之間互相連接，在傳輸與接駁過程中，無可避免帶來很多額外的安全風險，而這些安全風險往往並非來自本身的系統，而是來自外方，若然不小心將之忽略，便有可能殃及自身系統的安全性，並為黑客入侵打開方便之門。

因此，只有認識到系統相互依賴性，警惕到有「第三方」安全風險的存在，才能對症下藥，有效維護、改善與提升自身系統的安全性。筆者認為，無論是國泰航空、英國航空與轉數快三宗資訊保安紕漏事故，這一點是最值得記取的教訓。

最後一提，國泰航空在900多萬客戶資料外洩事故發生後，約半年才把事件公開，難怪受外界批評，反觀英航，事故發生後兩天，便馬上向外公布，有關資訊保安事故的信息披露和政府制訂安全標準等問題，也是一個很值得分析的問題，囿於篇幅，筆者另文討論。

〔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〕