【解牛集】— 刊於〈信報〉，2019 年 2 月 25 日

網絡保安「雙重道德風險」陷阱

許佳龍

科大資訊、商業統計及營運管理學系講座教授

生產力促進局屬下的「香港電腦保安事故協調中心」不久前透露，該中心去年共處理了 10,081 宗網絡保安事故，較上年增逾 50%，增幅相當凌厲。作案人透過殭屍網絡攻擊、惡意軟件及釣魚網站向受害者——包括企業或個人進行侵害或敲詐。據該中心解釋，保安事故去年之所以遽增，原因之一，是黑客幫助其他缺乏相關技術的犯罪分子提供一站式攻擊服務，降低了犯罪門檻，令殭屍網絡攻擊案件數量大增，可見網絡保安風險在當下以至可見未來都會有增無減，需要及早有效處理。

無可否認，在今日社會，無論個人或企業幾乎每一刻都離不開網絡，而企業或個人在網絡上往往都連接了或多或少的智能設備，從打印機到 Wi-Fi 路由器等。如果缺乏安全保障措拖，則物聯網中每一個部件，都可能成為犯罪份子作案的切入點。據全球網路安全巨頭 BeyondTrust 公司的評估，物聯網設備在 2019 年將成為惡意軟件攻擊的主要目標。事實上，物聯網如今無處不在。置身各處的隱形感應器和芯片無時無刻不在相互通信，傳輸和修改數據，因此，在如此複雜和瞬息萬變的環境下，怎樣確保網絡安全，顯然不是單一方能夠隻手包辦完成。

第三方風險外漏洞

記得筆者曾在本欄提出網絡攻擊與「第三方」風險問題。譬如，企業自身的網絡系統相當安全，但是，當這企業增加了一些由外判供應商（第三方）提供的額外服務時，便可能從外而內引入了可能的潛在安全風險。一旦「第三方」的系統安

全性出現了漏洞，黑客便可以乘虛而入，順藤摸瓜，直闖企業的網絡系統，為所欲為。

以英國航空公司的訂票網站遭黑客入侵為例，該公司廿多萬名透過信用卡付款的客戶個人資料外洩，遭黑客盜取。網絡漏洞的缺口，便在於收取信用卡的服務系統，其網頁出現了安全紕漏，以致在讀取信用卡付帳的過程中，為黑客所截取。這是「第三方」風險的紕漏。可以說，企業與企業之間、企業與用戶之間，甚至用戶與用戶之間，大家互相勾連，這種千絲萬縷的網絡關係，使網絡保安無可避免帶有相互依賴的「集體性」，很難單靠一方獨力完成。因而，我們也可以從責任分布的角度，去檢視網絡安全問題，令網絡安全得到更全面、更現實的「整體性」維護。

事不關己己不勞心之害

對於網絡安全，一般人很自然把保安視為網絡保安供應服務商的責任；甚至用戶也很自然地認為，這是企業的責任，它們有責任去設置一切保安設施，與自己無關。但是，除了第三方風險外，大家其實必須考慮到用戶與用戶之間互動的風險因素。事實上，用戶是網絡保安工作成果裡一個重要部分，是牽涉其中的「持份人」，在安全的維護上也有一定責任。

看深一層，在學術研究上我們認識到，若干工作的結果，往往需要由勞資雙方共同付出，攜手完成。在觀察和分析這種相互作用的行為，學者提出一個「雙重道德風險」（Double Moral Hazard）概念。須要說明一下，在信息經濟學裡，當市場參與者之間存在信息不對稱情況下，便會出現一種所謂的「道德風險」（Moral Hazard）。簡言之，市場參與者的經濟行為，在最大限度增進自身的效用時，卻忽略了對他人的影響。譬如，保險公司無法確知汽車保險購買者在買入保險後的行為，駕駛者購買了保險，基於車輛的損失由保險公司負擔，因而駕駛者便減少在駕駛時對路面交通安全的注意程度，從而使行車風險提高，增加保險公司低估風險的可能損失。

在「雙重道德風險」的視角下，假如某一項工作需要勞資雙方共同付出努力或投入，大家合力完成，雙方因對方也要付出，結果便減少了自身投入或付出的部分，導致整體結果未如理想。

「雙重道德風險」陷阱

事實上，在網絡保安方面，很多事故的肇因，往往就是因為大家墮入了這個「雙重道德風險」陷阱之中。很顯然，用戶是牽涉保安工作結果的一份子，於是企業難免認為，用戶會為保安出一分力，自己也會作出一些保護措施，譬如保護好自己的密碼；與此同時，用戶則認為，企業會做好防範網絡攻擊的措施和裝置，自己毋須多此一舉，結果，雙方都減少了對保安的警惕性和付出，為網絡攻擊者帶來侵入的黃金機會。

可以說，資訊保安要獲得良好成效，取決於企業和用戶兩者的付出和投入，而無法由單方獨力有效完成。目前，資訊保安事故頻仍，往往是因為忽視了用戶投入或付出的部分，這一點很值得清楚指出來。換言之，社會需要重新檢視一下用戶在網絡保安上所扮演的角色和責任。

目前，大部分企業的網絡安全裝置都有防火牆、抵禦木馬程式的防毒軟件裝置，即使如此，但假如用戶方隨意把自己的密碼與人分享、或與其他人共用電郵或已登入的電腦，則企業無論做了多少安全措施，也屬徒然。因為網絡安全的漏洞，可以在一個電郵中，便成為黑客攻擊切入之門。

Target 遭外部風險株連

很顯然，企業除了做足網絡安全的裝置和措施，還需要提出誘因，去激勵企業內員工做好自身保安付出和投入的部分。因為如果他們付出的部分不足，往往便會成為整個保安系統「致命」的阿基里斯腱(Achilles' heel)。

如何避免墮入這個「雙重道德風險」陷阱，筆者在一篇即將發表的論文《Bilateral Liability-Based Contracts in Information Security Outsourcing》（基於雙邊責任的信息安全外包合同）中，提出以合同的形式，來釐訂保安工作的責任分布。事實上，在網絡保安的責任和後果上，用戶都應該分擔其合理的投入或責任的部分，此舉對強化保安的效果產生積極作用，因而加強用戶在網絡保安工作的責任意識，筆者認為相當重要。

記得 2013 年聖誕零售旺季期間，美國零售業巨頭 Target 的「銷售時點情報系統」（Point of Sale, POS)遭黑客攻擊，以億計用戶的的銀行卡資訊被盜走，包括卡號、用戶姓名、通信地址、電話號碼、電子郵件等資訊，造成美國歷史上最嚴重的資訊洩露事故之一，三分之一美國人受到波及。後根據調查，Target 網絡系統之所以受到攻陷，關鍵是黑客首先攻入了 Target 一家外判供應商的網絡，再以此為切入點，侵入 Target 公司的網絡系統，而這家外判服務供應商遭到黑客成功攻擊，原因是該家外判供應商內一名員工中了「釣魚」病毒。

值得指出的是，Target 的電腦保安系統曾向員工提出警示，但因為有員工輕心，缺乏自己也有保安責任的意識，以致輕易地讓黑客入侵並為所欲為，鑄成了無法挽救的大錯。由此可見，用戶或企業內員工的網絡保安責任意識，在整個保安過程和結果中都十分重要，絕不能掉以輕心。

擺脫「雙重道德風險」陷阱

總體來說，在網絡保安上，除了需要留意「第三方」風險外，用戶在保安工作上的配合和支持，不可缺漏。很顯然，用戶需要認識自身在網絡保安上的角色和責任。若然對於「釣魚」電郵和訊息的警惕性不足、隨意把自己的電腦密碼寫在紙張上，或用簡單的生日日期數字作為密碼、把網絡保安的責任完全交給企業，沒有做好自身的保安投入或付出，往往為黑客打開入侵攻擊缺口。事實上，大部分的網絡攻擊事故，缺口都多在用戶方身上。如個別用戶的電腦受到病毒感染後，變成黑客長驅直入企業系統之門。

事實上，在現實環境裡，當用戶或員工不小心打開了一則「釣魚」電郵，並按照

指示，不問究竟，馬上「更新」個人的資訊或密碼，此舉隨即成為黑客據此入侵企業網絡系統之門。面對這種情況，如今也有一些企業為了嚴防員工「引狼入室」，在網絡保安上，往往自家向員工發出「釣魚」電郵，以測試員工對此的警惕性，若有員工粗心大意「中招」，這名員工便需要接受網絡安全的「再培訓」。但畢竟這種做法顯得相當被動，絕非長治久安之策。很顯然，關鍵而徹底的做法，是要避免參與網絡保安工作的各方持份者墮入「雙重道德風險」陷阱，並且明確和讓用戶清楚認識到自己在網絡保安上的角色和責任。這一點，在當前網絡犯罪不僅增量而且作案手法也層出不窮的情況下，顯得尤其重要，而且更是有效減少或堵塞網絡保安漏洞的「不二之門」！

〔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〕