Cloud Computing

資訊安全之重要性：網際 / 隱私

Information Security Matters Cyber/Privacy

作者: Steven J. Ross, CISA, CISSP, MBCP,

is executive principal of Risk Masters International LLC. Ross has been writing one of the *Journal*'s most popular columns since 1998. He can be reached at *stross@riskmastersintl.com.*

譯者:**劉其昌,**中華民國電腦稽核協會編譯出版委員會委員、立法院教育及文化委員會主任秘書

在過往的一年間或者左右之時間裡，有兩次我收到更換過之信用卡，因為是依據信用卡之廠商家們所已經宣告之信用卡使用之失效時間數字，我時常遇到這種情廠商家門。而每一次更換信用卡事件，皆會導致我花用大約一個小時之時間用以搜尋研究我的信用卡之消費紀錄，瀏覽我曾經使用信用卡支付消費活動的消費廠商之網頁，同時更新我的消費紀錄。當然我絕對不會是唯一那些已經受到影響的人，在這邊所受到影響的人可能是我所損失時間成本的 7 千萬倍，而在另一方面可能是我所損失時間成本的 4 千萬倍，不過將這些損失時間成本累加起來，它遲早是會造成相當程度之實質不方便的。

上述遭受質疑之廠商家們不是僅僅喪失它們對於消費者顧客之紀錄，同時我的消費信用資訊亦遭它們印刷而公諸於媒體，廠商家們已遭網路犯罪者所欺騙，網路犯罪者已深入它們的作業體系，偷竊包括我在內地數以百萬計之其他消費者之消費資訊，換言之，廠商家們已遭受網際網路之犯罪攻擊，所有的注意力應集中於這類網路犯罪，在此我完全關注於資訊之安全議題。

原先和衍生而出之衝擊

當資訊遭受偷竊之後，它會產生事件原先和衍生而出之衝擊，就前者之類型而言，某些資訊之本身就具有原先之價值，例如:書籍和電影編劇它們本身就具有原創之價值，(當日本新力公司去年遭受網路之犯罪攻擊時，據有關之報導指出，網路之犯罪攻擊除了徹底癱瘓必要之維運系統，和公開發布令人困擾之電子郵件內容以外，網路之犯罪者尚且偷竊一些電影之膠捲，我實在被這些網路犯罪攻擊者之思維所驚嚇住---而這絕大部分應歸屬於那些北韓人們----他們聚集圍在一起正觀看著 Annie 影劇[1]。

的確任何遭竊之信用卡上數據必然會具有某些原本之商業價值，因為當竊賊將所偷竊之信用卡上之數據銷售於其他之罪犯，同時當其他罪犯們使用尚未到期之信用卡進行商品勞務之購買消費時[2]，當竊賊是盜取現金卡時此一資訊將可使竊賊重他人之帳戶中盜領現金，這些都是所謂的因網路犯罪後所衍生出之間接衝擊效果。網路之犯罪者們一旦竊取信用卡之資訊就可以為它們自己創造出任何具有實質價值之產物，而從我個人地觀點角度來看，其總和之淨效果就是導致當事人之不方便。不過若從比較深一層地觀點來看，他係對我個人財務隱私之嚴重侵犯，目前我還未大幅度看到公開之討論文獻中有涉及認知網路犯罪係針對個人財務隱私之嚴重侵犯地論述，大多數已廣為公開之網路犯罪攻擊文獻尚未以侵犯個人之財務隱私作為大夥討論之焦點[3]。

一般公認接受之隱私原則

一般公認接受之隱私原則[4]對於資訊之隱私內容定義有一個明確之敘述內容，他將資訊之隱私內容定義為”個人和組織團體所擁有攸關其個體本身有關資訊之蒐集、使用、保存、公開揭露、刪除回復等之法定之權利與義務”，考慮網路犯罪攻擊者對於信用卡持有者之財務隱私之侵犯所已經造成的嚴重程度時，或許一般公認接受之隱私原則能夠提供若干之洞察機制，用以保護避免財務隱私遭受網路犯罪之侵害攻擊，這大約有十個原則可供參考。

原則 1: 管理能力

有關資訊之隱私它必須是一個擴及整體企業範疇之政策，同時在組織結構之中保有一定暢通之管道連結，為防止破壞資訊隱私及其所衍生之問題，當局必須明確地任命指定專人負責此一問題[5]，諸如設置隱私權主管(CPO)，其實我本身對於隱私權主管並不完全了解其職責工作，有關他在執行網路安全任務時所扮演之領導角色為何?相反地我倒是十分樂意和他們保持溝通與互動。或許一般公認接受之隱私原則能夠就此一情況加以擴大延伸，要求應設置專責之網路安全負責機關，此一任命地用意之一為達成研發確保網路資訊隱私安全，不會遭致網路攻擊竊取風險之方法。

原則 2: 通報能力

組織團體可推定當欲蒐集、使用、保存、公開揭露有關個人屬性之資訊時，必定要善盡其通報之責任與義務，吾人可以相信在社會上不會有人說:”我們將會收集你地信用卡資料後用以交付網路罪犯使用”比較合宜地看法是，我們已經獲得潛在地共識，那就是信用卡之發卡廠商或者是已知訊息之銀行，會在適時之時間以電子郵件之方式通知我新的信用卡應該已經可供使用。

原則 3: 選擇和同意

當然吾人針對我的信用卡之資訊是否已遭受網路竊取之事件沒有任何之選擇餘地，但是我們擁有一個選項那就是是否應到無法保障我們信用卡資訊安全的商家去進行消費，顯然地，當發生幾個主要的重大網路竊取信用卡資訊之後，消費者不會與他們自己的口袋作對，重而選擇其他可確保消費資訊安全之其他廠商進行消費[6]。

原則 4: 資訊蒐集

信用卡廠商們所蒐集之消費信用資訊，其用途當然不同於網路犯罪者之使用目的，但是信用卡廠商們所使用之資訊體系之安全程度，以及保持之態度是否真正了解可能產生之風險?對於擁有個人資訊之系統，在處理上應該以最嚴格緊密之安全等級加以處理才是。

原則 5: 資訊使用、保存及棄置

我持有之信用卡大致上用於購買我的消費事務，假若與信用卡相關之資訊遭受竊取時，如在一個銷售點(POS)裝置上偷竊一張信用卡，此時並未違反資訊隱私之保護原則，但若廠商將大批未經加密保護之資訊檔案，未以妥善之方式加以保管處理，以不正當之方式態度棄置處理這些資訊時，將會違反保護資訊隱私之安全原則。不幸地是，雖然從技術面之資訊明細顯示，有若干重要地零售面網路犯罪攻擊行為，其實充其量而言亦尚不具完備性，不過從已印製之書面報告報導指出，零售端銷售終點以及其間之網路

下述資訊系統之可責性並非系統安全性欠佳，而是其軟體層面之不足。

伺服器等，將是已經遭受網路攻擊入侵之主要對象源頭。

原則 6 及 7: 接取與公開至第三者團體

吾人致力於接取、檢視、和更新有關自我本身之資訊事宜，係與資訊網路之犯罪沒有任何之關聯性，同時在一般公認接受之隱私原則下，在其符合之規定框架中，盡量調適是符合其原則之條件下，所計畫準備公開之任何資訊亦與網路之犯罪無關，但是我質疑這個是不是一般公認接受之隱私原則作者原先所指之本意所在。

原則 8: 隱私之安全性

在應用於網際網路之犯罪方面，網路隱私之安全性原則的確完全是係一般公認接受之隱私原則作者們所牢記於心地，如何防杜任何未經合法授權，無論係經過實質或是抽象邏輯方式接取資訊時皆應極力避免，但顯然當今之資通訊產業在實務上是未能做到地，當吾人檢視所有已經發生之網路攻擊事件時，它似乎顯示著當使用完備地控管接取資訊之機制系統，將會使得接取資訊之忠實程度更為忠實，而如何致力於防杜阻止已充分準備且以竊取網路資訊為職責者，經驗證實其有效性將會如歷史上之馬其諾防線班地發揮效果(未來之文獻中將會有更多這方面文章之討論)。

原則 9:安全品質

依據一般公認接受之隱私原則作者們所定義之資訊安全品質係指，如何確保維護”個人相關資訊之正確性、完整性、和攸關性”，這雖然不是我所欲表達意義所用之名詞，卻是當前在面臨網路安全攻擊之年代中，我所該應用於防杜網路隱私犯罪時所適用之原則，正如我先前所已經寫述的，我們相信在吾人所討論之資訊系統之易受攻擊之弱點處，不在於其安全性之次佳，端在於其軟體本身之不適當不充足[7]。

原則 10: 監督和執行

依據媒體之報導再竊取重要個人資訊中，最令人為之生氣地主要論點之一是，在相當多之情況裡，組織機構在遭受網路入侵攻擊之損失，即使在企業組織已知係了解後，其發生仍是一段漫長之期間，就再舉一個例子來說，美國人事管理部門辦公室(OPM)在 2014 年 7 月間告知人事人員，在該年之 3 月間發生個人資訊紀錄遭受網路入侵之攻擊事件[8]，其後怠至 2015 年之 6 月間人事管理部門辦公室再度宣稱其人事資訊資料有 4 百萬筆之記錄遭受網路攻擊而被竊取，復至同年之 7 月間，遭受網路竊取之個人資料已攀升至 2 千 1 百 5 十萬筆個人資訊紀錄[9]。我並無法精確地知悉了解上述資訊是如何發生遭致攻擊者網路入侵，但我可以確信事實上有人已經注意到，當一旦發生網路入侵攻擊事件時，在那期間他是持續不斷地在進行當中。而在發生入侵之當下為阻止網路入侵行為目的之技術其實是已存在地，唯顯然這些防杜入侵技術是沒有被有效率地使用，因為電腦系統本身是太陳舊了[10]。

結語

當考量網路攻擊侵犯個人隱私權之議題時，事實上有相當多地內容應當被學習，而一般公認接受之隱私原則作者們雖提供若干之指導原則，但是該等原則未必能與網路上現行竊取個人資訊之行為態樣完全十足吻合，而機構組織是否能完全適用吸收這些經驗教訓哪? 這些也只有留待以後才能真正看見了解。

END NOTES

1 Sakoui, Anousha; "Sony Films 'Fury' and 'Annie' Said Stolen in Cyberattack," Bloomberg Business, 29 November 2014, *www.bloomberg.com/news/articles/2014-11-30/sony-films-fury-and-annie-said-stolen-in-cyberattack*

2 Hackett, Robert; "Online, a Bazaar Bursting With Stolen Credit Card Information," Fortune, 21 September 2014, *http://fortune.com/2014/09/21/home-depot-stolen-cardinformation-market/*

3 Interestingly, the *Preliminary Cybersecurity Framework* issued by the US National Institute of Standards and Technology contained a section on a "Methodology to Protect Privacy and Civil Liberties for a Cybersecurity Program" that was eliminated in the final version issued in February 2014.

4 American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA), Generally Accepted Privacy Principles, August 2009. ISACA® and the Institute of Internal Auditors were also contributors to this document.

5 *Ibid*., p. 13. The document referenced here is the version for business people, not the one for accounting practitioners.

6 For example, see Target, "Target Provides Update on Data Breach and Financial Performance," press release, *http://pressroom.target.com/news/target-provides-updateon-data-breach-and-financial-performance.*

7 Ross, Steven J.; "Microwave Software," *ISACA® Journal*, USA, vol. 1, 2015

8 Email reproduced in the *Washington Post*, "E-mail to OPM Staff on Security Breach," 10 July 2014.

9 Bisson, David; "The OPM Breach: Timeline of a Hack," Tripwire, 29 June 2015, *www.tripwire.com/state-ofsecurity/security-data-protection/cyber-security/the-opmbreach-timeline-of-a-hack/*

10 C-SPAN, Testimony by the Office of Personnel Director Katherine Archuleta, *www.c-span.org/video/?326767-1/opm-director-katherine-archuleta-testimonydata-security-breach*

Quality Statement:
This Work is translated into Chinese Traditional from the English language version of Volume 1, 2016 of the ISACA Journal articles by the Taiwan Chapter of the Information Systems Audit and Control Association (ISACA) with the permission of the ISACA. The Taiwan Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.

品質聲明：
ISACA臺灣分會在ISACA總會的授權之下，摘錄ISACA Journal 2016,Volume 1中的文章進行翻譯。譯文的準確度及與原文的差異性則由臺灣分會獨立負責。

Disclaimer:
The ISACA Journal is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the ISACA Journal.

Opinions expressed in the ISACA Journal represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute and their committees, and from opinions endorsed by authors' employers, or the editors of this Journal. ISACA Journal does not attest to the originality of authors' content.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, MA 01970, to photocopy articles owned by ISACA, for a flat fee of US $2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

免責聲明：
ISACA Journal係由ISACA出版。ISACA 為一服務資訊科技專業人士的自願性組織，其會員則有權獲得每年出版的ISACA Journal。

Cloud Computing