

將行動支付視為一個安全控制？

Mobile Payments as a Security Control?

作者：Robert Clyde, CISM
Is managing director of Clyde Consulting LLC (USA). He also serves as a director on the boards of White Cloud Security (trusted app list enforcement); TZ Holdings (formerly Zimbra), a leader in community and collaboration software; and Xbridge Systems, a leader in data discovery software. He chairs a board-level ISACA® committee and has served as a member of ISACA's Strategic Advisory Council, Conference and Education Board, and the IT Governance Institute (ITGI) Advisory Panel. Previously, he was CEO of Adaptive Computing, which provides workload management software for some of the world's largest cloud, high performance computing (HPC) and big data environments. Prior to founding Clyde Consulting, he was chief technology officer at Symantec and a cofounder of Axent Technologies. Clyde is a frequent speaker at ISACA conferences and for the National Association of Corporate Directors (NACD). He also serves on the industry advisory council for the Management Information Systems Department of Utah State University (USA).

譯者：譚家蘭，國立政治大學會計學系特聘教授，電腦稽核協會專業發展委員會委員/編譯出版委員會委員

詢問每一個商人，他們都會告訴你，接受信用卡付款將會帶來安全方面的挑戰。除了要擔心支付卡產業資料安全標準 (PCI DSS) 的要求外，作為商業環境中的安全專業人士，還有許多其他事情也引起關注。這些事情包括了，對於潛在的舞弊交易保持警覺、記錄持卡人數據的存儲位置以及數據在商家環境中的路徑、確保持卡人數據環境 (CDE) 與其他環境之間的適當劃分、評估服務提供商的安全和合規狀況以及其他許多議題。

關鍵是，從安全角度來看，付款可能是具有挑戰性的。由於沒有人擁有無限的預算，因此安全從業者的責任是以具預算意識和注重效率的方式找出创新的手法來應對這些挑戰。在這種情況下，創造性往往意味著有時看起來似乎是非正統的方式來擠壓每一點效用的機會，以提供自己提升安全利益的機會，同時確保這些機會對業務運營的影響最小。

相信與否，接受行動支付可以是一個這樣的大道。通過了解行動支付的工作原理，並尋求創造性的方式將其從安全角度看成是一個優勢，利害關係人可能會採取幾個步驟來推動他們的安全計劃，同時提供一個有價值的服務給客戶。

為何行動支付？

坦白說，這個說法對許多從業者

來說可能聽起來很瘋狂。例如，ISACA2015 年的行動支付調查顯示，在接受訪問的 900 名安全從業人員中，有 87% 的受訪者預計明年行動支付數據的洩露將會有所增加。大約一半 (47%) 的受訪者表示行動支付不安全，只有 23% 的受訪者表示行動支付在保護個人信息方面是安全的。所以很明顯地，這個行業是以懷疑的態度來看待行動支付。

也就是說，行動支付的替代方案是值得考慮的。隨時琢磨舞弊和濫用的渠道，每次客戶出示卡片以啟動卡片交易。只要卡片不在持卡人的錢包裡，卡片就有機會丟失或被盜。通過銷售點 (即通過過濾器) 進行截取是有可能的，銷售點 (POS) 本身的邏輯存儲提供了竊取的機會，POS 和任何系統手之間網絡嗅探的可能性支付細節退款到付款處理後端等。在這條路上的每個步驟，事情都可能會大錯特錯。

現在，將其與 Android Pay、Samsung Pay 或 Apple Pay 等行動支付方式進行比較。在這些模型下，主帳號 (PAN) 通過行動支付憑證代碼化進行保護，交易時使用強化密碼進行身份驗證，並且有一些機制來減輕或甚至消除傳統卡片可能遇到的許多舞弊情況。此外，在可以開始支付之前，透過補充認證 (生物識別號碼或個人識別碼 [PIN])，持卡人和支付交易本身之間的要求具有強大的約束力。

普遍來說沒有人會認為行動支付具有更強大的安全性，但是行動支付與傳統的信用卡交易相比具有相當多的優勢。行動支付的接受度在未來很有可能會從挑戰變成機會。

實務上的風險抑減

考慮到行動支付的安全性問題，有什麼方法可以改善行動支付的問題並使行動支付愈來愈受安全專家歡迎？首先我們要先瞭解行動支付所擁有之安全特性並找出潛在的優點及缺點。瞭解行動支付不代表我們需要像閱讀工程規範一樣仔細，但是瞭解行動支付可以幫助安全專家更認識它的概念，以致於他們可以對行動支付做出風險決策。在國際電腦稽核協會所發佈的白皮書，手機是不是安全支付的贏家？簡介了企業價值建議及描述了一些可以提高安全性的控制方法。

白皮書中有提到一些細節，行動支付的其中一個重要的優點是資料記號化下卡號及帳號(PAN)並不會儲存在手機中或是把資料傳到商人手中。就算商人的網絡妥協，卡號及帳號(PAN)也不會妥協，因此可以降低失竊及舞弊的風險。

這是一個很好的起點，但是行動支付也可以從其他方面提高安全性的價值：具體地說，因為行動支付接受度的發展需要位於零售點之POS系統的同步更新，此更新可以提供機會來從新造訪這些零售點並同時使用較廣闊的視野來看針對安全的相對措施。(因為商人會告訴你，零售點常常是挑戰發生的地點)

結合有系統的再訪各零售點的安全措施—與POS系統及地點有關—有幾個優點。為了完成PCI DSS系統下的文件(大零售商需填寫Report on Compliance [RoC]，小零售商需填寫Self-Assessment Questionnaire [SAQ])，這些零售點的子集會經過一些調查。具體地說，因為零售點所牽涉到的一些支付交易一般都是CDE的一部分，他們通常會包含在評估中。這代表更新POS系統的預算可以同時滿足兩個目的，使POS升級(讓已

存在的風險移轉)並製造更廣的機會來再訪其他地區。

行動支付的接受度明顯的是一個挑戰並同時具備新科技不容易被理解的特質。但是，它同時代表著給精明專家的機會，專家知道自己需要的是什麼—就像柔道專家—可以把逆境變成轉機。

Quality Statement:

This Work is translated into Chinese Traditional from the English language version of Volume 4, 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 4 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。

Copyright

© 2016 of Information Systems Audit and Control Association (“ISACA”). All rights reserved. No part of this article may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system, or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise), without the prior written authorization of ISACA.

版權聲明：

© 2016 of Information Systems Audit and Control Association (“ISACA”). 版權所有，非經ISACA書面授權，不得以任何形式使用、影印、重製、修改、散布、展示、儲存於檢索系統、或以任何方式(電子、機械、影印、或錄影等方式)發送。

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。

ISACA Journal收錄的文章及刊物僅代表作者與廣告商的意見，其意見可能與ISACA以及資訊科技治理機構與相關委員會之政策和官方聲明相左，也可能與作者的雇主或本刊編輯有所不同。ISACA Journal 則無法保證內容的原創性。

若為非商業用途之課堂教學，則允許教師免費複印單篇文章。若為其他用途之複製，重印或再版，則必須獲得ISACA的書面許可。如有需要，欲複印ISACA Journal 者需向Copyright Clearance Center(版權批准中心，地址：27 Congress St., Salem, MA 01970) 付費，每篇文章收取2.50元美金固定費用，每頁收取0.25美金。欲複印文章者則需支付CCC上述費用，並說明ISACA Journal 之ISSN 編碼(1526-7407)、文章之出版日期、卷號、起訖頁碼。除了個人使用或內部參考之外，其他未經ISACA或版權所有者許可之複製行為則嚴明禁止。