Summer 6-27-2016

AN APPROACH TO RISK MANAGEMENT FOR E-COMMERCE

Sadhna Sharma
National Chiao Tung University, sadhna.sharma23@gmail.com

Cheng-Yuan Ku
National Chiao Tung University, cooper.c.y.ku@gmail.com

Yung-Ting Chuang
National Chung Cheng University, ytchuang@mis.ccu.edu.tw

AN APPROACH TO RISK MANAGEMENT FOR E-COMMERCE

Sadhna Sharma, Institute of Information Management, National Chiao Tung University, Hsinchu, Taiwan, sadhna.sharma23@gmail.com

Cheng-Yuan Ku, Institute of Information Management, National Chiao Tung University, Hsinchu, Taiwan, cooper.c.y.ku@gmail.com

Yung-Ting Chuang, Department of Information Management, National Chung Cheng University, Chiayi, Taiwan, ytchuang@mis.ccu.edu.tw

Abstract

Today's trend of online shopping proves the vital role e-commerce plays in our daily life. Online transactions require reliable networks, and reliable networks depend on secure information technology. These networks have many advantages, but they have disadvantages as well—notably, the need for risk management. The growing importance of e-commerce, with its associated need to ensure trust in online transactions, has led the authors to study and propose risk management in e-commerce from a holistic perspective, thus enabling the implementation of real-time auditing of e-commerce transactions using the digital agents' technology. In this paper, the authors discuss e-commerce's risks and present a methodology that can be used to manage those risks. It concludes that e-commerce risks are a high priority for online businesses, and that many of the requisite controls are extensions of controls for managing risk in other information systems.

Keywords: Risk management, network computers, e-commerce, information system risk

1 INTRODUCTION

Electronic commerce or e-commerce is the buying and selling of goods and services. It's very popular to buy anything and pay online, transmitting funds or data over an electronic network, primarily the internet. These business transactions occurs business-to-business, business-to-consumer, consumer-to-consumer or consumer-to-business. The terms e-commerce and e-business are often used interchangeably. Nowadays people are not going to the shops to buy things but rather checking the details and pictures of the product on a device, then ordering and paying online; after a few days, the seller will deliver that thing to your door. Electronic commerce is a process that enables sale or purchase of goods and services over computer networks with methods designed for this purpose (WTO, 2013). Although orders can be made electronically, the delivery of goods, services or payments is not limited to the online world. E-commerce transactions can occur between businesses, households, individuals, governments and public or private establishments (OECD, 2011). E-commerce has some advantages, most notably the ability to save time and offer buyers and sellers a wider range of price and quality, but we can't avoid e-commerce's disadvantages. Security is the main concern in online shopping. Because of security, buyers are scared to buy items online, and this affects e-businesses. The success or failure of an e-commerce business depends on these security and privacy issues (Tripathy and Mishra, 2013), and users' trust is essential for development in e-commerce (Rand and Meshram, 2012). E-commerce generally is made by using some combination of telephone, fax, TV, computers, the internet, electronic payments, money-transfer systems and electronic data interchange. In this study, we only consider electronic commerce transactions that are made via the internet.

Most of the buyers using the internet buy items from around the world using e-commerce, which can be used business-to-business, business-to-consumer, business-to-government, consumer-to-business, consumer-to-consumer, consumer-to-government, government-to-government, government-to-business and government-to-consumer, as shown in Figure 1. Business-to-business is the e-commerce relationship between organizations; business-to-customer is the provision of service by a business to a consumer; customer-to-customer is the e-commerce relationship among consumers.

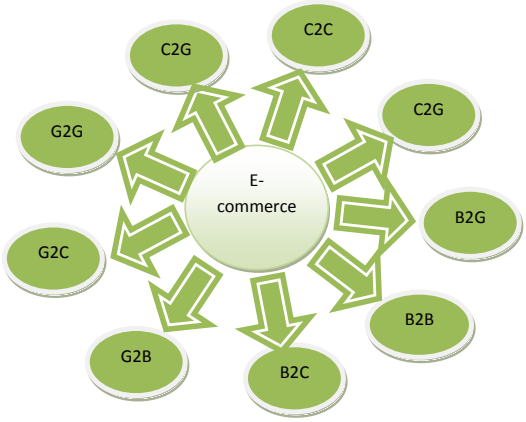

Figure 1. E-Commerce Classification

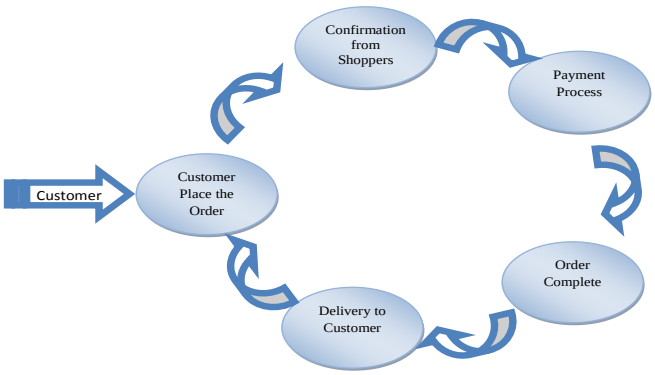

Figure 2. Online Completed Transaction steps

Although e-commerce provides a 24/7 unlimited shopping platform, security remains a primary concern for all customers. There are many issues, in fact: anonymity of merchants, misrepresentation of products, consumer fraud and security problems (Niranjanamurthy et al, 2013).

From order to delivery, e-commerce transactions have a cycle and there are many points of risk throughout every online transaction. Figure 2 shows the steps of an online transaction. This paper seeks to resolve a range of issues in e-commerce security. Many countries are currently trying to make e-commerce more reliable and solve these problems via regulation.

2. EVALUATION OF E-COMMERCE

E-commerce is also improving business interactions. It facilitates the network form of organization where small, flexible firms rely on partner companies for supplies and distribution to meet changing customer demand more effectively. Over the past 20 years, e-commerce has grown rapidly, offering advantages to both businesses and consumers since the first e-commerce transaction in 1995 (Laudon and Traver, 2013). As changing regulations lower barriers to ecommerce, it is expected that e-commerce will continue to evolve in the future. The spread of internet access and the rising expectations that come with it are two of the main drivers of the development of e-commerce. New internet users come online every second; currently, about 40% of the world's population has an internet connection.

Users Growth	% of World Population with Internet(Penetration)	Year
12.2%	25.6	2009
16.1%	29.4	2010
11.7%	32.5	2011
10.5%	35.5	2012
8.0%	37.9	2013
7.9%	40.4	2014

*Table 1. Internet use in the world (*Internet Live Stats, 2015)

In 1995, that figure was less than 1%. The number of internet users increased tenfold from 1999 to 2013. The billion-user mark was reached in 2005, the two-billion mark in 2010, the three-billion in 2014. Figure 3 shows the number of global internet users per year since 1993 (ITU 2014).

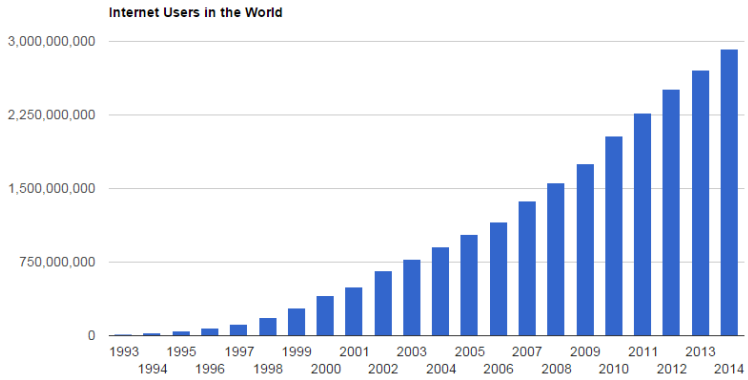

Fig 3: Internet Users in the world (ITU 2014)

Global e-commerce sales have gradually increased. In 2014, e-commerce sales increased by 21% compared to the previous year. It is expected that global e-commerce sales will increase over 10% every year and reach $1.506 billion in 2018. When one considers the size of the online market, consumer behavior, growth potential and infrastructure, the USA, China and the United Kingdom are the top countries in e-commerce around the world (ATKearney, 2015).

3. RISKS AND SECURITY IN THE WAY OF E-COMMERCE

The success or failure of an e-commerce business depends on security and privacy (Tripathy and Mishra, 2013). Users' trust is essential to business development (Rane and Meshram, 2012). With the popularization of electronic payment, security issues have become a key problem. Theft of personal data (privacy) and unauthorized access (security) are serious issues in e-commerce for customers and service providers alike. Privacy is the ability of an individual to control the terms under which their personal information is acquired and used (Culnan, 2000). An individual's privacy, as such, is always in an inherent state of tension, since it must be defined in conjunction with the capabilities of others to

transact business and even to control their own privacy. Customers are concerned about the risk of reuse of their personal data for unrelated purposes without their consent. This includes sharing with third parties who were not part of the transaction in which the consumer related his or her personal data.

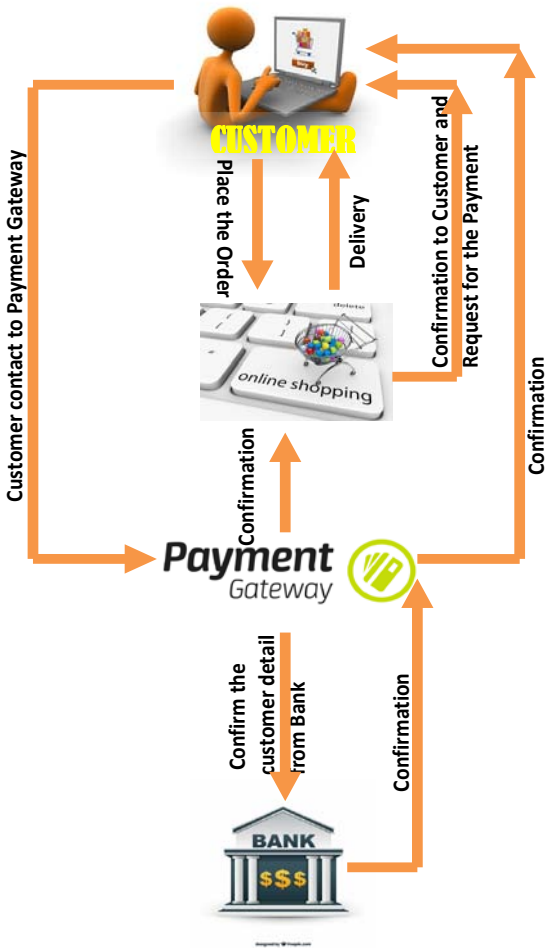

Figure 4. Steps of e-commerce business transaction

Risk in the different phases of e-commerce transactions shows that there are many factors to be managed (Yasin et al, 2012). Online providers are trying to pull more and more users to inflate their numbers, but users' privacy and security cannot be at stake. Thus, to improve their business situation, providers should be specific on their security strategies (Srikanth, 2012). Security is also a major issue for e-commerce sites and consumers alike. Consumers fear the loss of their financial data, and e-commerce sites fear the financial losses associated with break-ins and any resulting bad publicity. Not only must e-commerce sites and consumers judge security vulnerabilities and assess potential technical solutions, they must also assess, evaluate, and resolve the risks involved. There are many points of failure or vulnerabilities in an e-commerce environment. Even in a simplified e-commerce scenario – a single user contacts a single web site, and then gives his credit card and address information for shipping a purchase – many potential security vulnerabilities exist. The user's web browser connects to the merchant front-end. When a consumer makes an online purchase, the merchant's server usually caches the customer's personal information. However, security is not just a matter of technology; implementing technology without the proper organizational processes will not solve security problems. There are many critical social and organizational issues with security (Treese and Stewart, 1998).

A second problem is that software management is a substantially larger problem with security than with many other types of software. As mentioned, hackers constantly discover new vulnerabilities in

both new and existing systems. An underappreciated risk is that an insecure e-commerce server can undermine corporate regulatory compliance.

Understanding of security would be incomplete without an analysis of the underlying economic issues. The above security functions either as a technical imperative or as a set of social and organizational issues; however, it must be stressed that security for both consumers and sites requires an analysis with the proper weighing of potential risk. As Anderson points out, security engineering is a matter of control and power as well as access (Anderson, 2001). Security mechanisms can be used to govern compatibility and attempt to control network effects governing the adoption of new or potentially replacing technologies (Shapiro and Varian, 1999). Figure 4 shows an online transaction where, after the customer places the order with an online shopping hub, the hub sends the customer an order confirmation and a request for payment, the customer contacts the payment gateway and provides their bank information, the payment gateway contacts the appropriate bank to check the customer information, the bank sends the confirmation to the payment gateway, the payment gateway sends the confirmation to the customer and vendor, and finally the vendor delivers the order to customer.

4. RISK MANAGEMENT TO REDUCE THE E-COMMERCE RISK

Electronic payment is an easy, quick and cheap payment system based on electronic communication. Buyers and sellers do their deals without seeing each other. The rapid development of the internet brought e-commerce to public attention, and it was acknowledged to be full of potential. In e-commerce, there are many ways in which an unscrupulous person can cheat users. In the early days of the internet, the popularity of e-commerce hinged on whether data transfers could be made secure. Although the following options may not be helpful for ending risk in e-commerce, they may help to reduce it:

1. Training to team on e-commerce risks: Train your team in risk management policies and procedures, and the fraud and security risks involved in an e-commerce transaction. The more informed your organization is, the easier it will be to combat online threats and to carry out risk-mitigating measures.
2. Spread organizational policies to customers: Make sure your website provides guidance to customers in the form of your privacy policy, information security, shipping & billing policies, and refund policies. This is also helpful to avoid dissatisfaction and disputes.
3. Ensure Payment Card Industry (PCI) compliance: All e-commerce organizations are required to be PCI-compliant and must adhere to the rules outlined by the Payment Card Industry Security Standards Council. If your organization is not PCI-compliant, it may be exposed to severe fines and the loss of its payment ability.
4. Protect your e-commerce business from intrusion: Check the system for viruses and hackers, change passwords, make software updates, and check sensitive data on a regular basis to make the system secure for e-commerce transactions.
5. Know the details of your payment service provider contract: Be familiar with your contract, particularly the areas that refer to holding funds and chargeback liability. Know the length of time and conditions under which your deposits may be held, and know your liability for fraudulent transactions.
6. Make strict laws: Classify e-commerce fraud as a type of crime in which perpetrators interfere with e-commerce for the purpose of ill-gotten gains.
7. Privacy-enhancing technologies: Although there are many technologies used for surveillance, the technologies for forming agreements (contracting) about the release of private data, the technologies for labelling and trust, and privacy-enhancing technologies (PETs) should be much stronger.

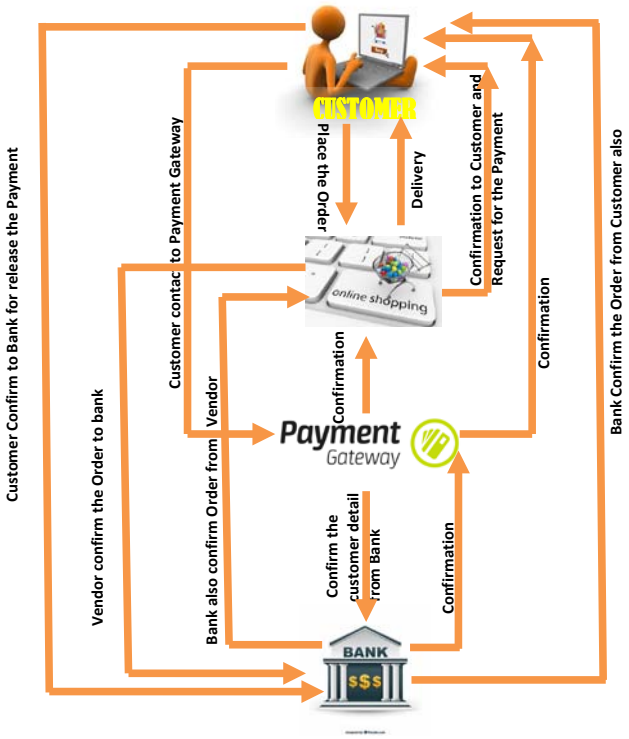

Figure 5. Secure transaction in e-commerce or online shopping

8. Encryption technology: Public-key systems, also called symmetric cryptosystems, use a common key to encrypt and decrypt information. The sender and receiver must have the same key in order for the system to work. The most famous public-key systems algorithm is Data Encryption Standard (DES). The public-key system, which is also called an asymmetric password system, uses two keys: one is used to encrypt, another for decryption. Each user has two keys: a public key and a private key. Users can send out a public key; because of the mathematical relationship between the two keys, anyone with the public key can encrypt data, but only a user with the private key can decrypt it. In order to guarantee the private key is kept secret, all users' keys should be self-generated. Cryptographic technologies can be used at various points in the payment system.

9. Digital signature: A digital signature is a cryptographic tag that only one author can calculate. The tag can be combined with any kind of data that the author might create, and the tag's validity can be checked by anyone who can access the data. A digital signature is the salient application of public-key cryptography, and is an analogy of a handwritten signature.

10. Digital envelopes: Secure Electronic Transaction, or SET, depends on a password system to ensure reliable transmission. The system uses a randomly chosen set of generated symmetric keys to encrypt data, and then sends the symmetric key, encrypted, to the recipient in a "digital envelope". The two datasets can be combined to decrypt the message.

11. Change Password: It is always recommended to change or alter one's password on a regular basis, and the password shouldn't be easy to guess.

12. Banks should confirm orders from payment gateways and customers as well: The steps in Figure 5 are not safe. Before releasing the payment, the bank should confirm the order with the legal payment gateway and the customer. When the customer and payment gateway send the order confirmations, the bank can release the payment to the vendor and the vendor can deliver the order as shown in Figure 5.

5. CONCLUSION

In the last few years, many researchers have offered solutions to the security and privacy issues that are the loopholes in e-commerce transactions. E-commerce includes the transmission and exchange of information, products, and services—online transactions and payment, and also resource-sharing between enterprises. In the effort to make electronic business secure, there are many problems to be solved beyond privacy and security. Beyond buyers and sellers, financial institutions, government agencies, certification bodies, distribution centers, and other organizations must contribute solutions. However, organizational policies and electronic signature technology may play as important a role in security and privacy as any other solution. Careful analysis will ultimately bring greater transparency and proficiency to the online process so that users can overcome risk and e-commerce can go on unhindered. This paper has proposed a set of guidelines for the benefit of users, so that those users can use online transactions in a safe and secure manner.

Acknowledgment

This research was supported in part by MOST 104-2410-H-194-090-MY2 of Ministry of Science and Technology, Taiwan.

References

Anderson, R. (2001, December). Why Information Security is Hard-An Economic Perspective. In Proceedings of the 17th Annual Computer Security Applications Conference, p. 358, IEEE Computer Society.

ATKearney, Global Retail E-Commerce Keeps on Clicking, https://www.atkearney.com/consumer-products-retail/e-commerce-index/full-report/-/asset_publisher/87xbENNHPZ3D/content/global-retail-e-commerce-keeps-on-clicking/10192, (2016/03/10)

Tripathy, B. and Mishra, J. (2013). Protective measures in E-Commerce to deal with security threats arising out of social issues - A framework. International Journal of Computer Engineering and Technology (IJCET), 4(1), pp. 46-53.

Culnan, M. J. (2000). Protecting privacy online: Is self-regulation working? Journal of Public Policy & Marketing, 19(1), pp. 20-26.

Internet Live Stats (2015), http://www.internetlivestats.com/internet-users/, (2016/03/10)

Laudon, C. K. and Traver, G. C. (2013). E-commerce 2013: business, technology, society. Pearson Education, 9th Edition.

International Telecommunication Union (ITU) (2014), Manual for Measuring ICT Access and Use by Households and Individuals, http://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ITCMEAS-2014-PDF-E.pdf, (2016/03/10)

Niranjanamurthy, M., Kavyashree, N., Jagannath, S. and Dharmendra, C. (2013). Analysis of E-Commerce and M-Commerce: Advantages, Limitations and Security Issues. International Journal of Advanced Research in Computer and Communication Engineering, 2(6), pp. 2360- 2370

OECD (2011). OECD Guide to Measuring the Information Society 2011, http://www.oecd.org/sti/ieconomy/oecdguidetomeasuringtheinformationsociety2011.htm, (2016/03/10)

Rane, P. B. and Meshram, B. B. (2012). Transaction Security for E-commerce Application. International Journal of Electronics and Computer Science Engineering, 1(3), pp, 1720-1726.

Shapiro, C. and Varian, H. R. (1999). Information Rules. Cambridge, MA: Harvard Business School Press.

Treese, G. W. and Stewart, L. C. (1998). Designing Systems for Internet Commerce. New York: Addison-Wesley

Srikanth V. (2012). E-commerce Online Security and Trust Marks. International Journal of Computer Engineering and Technology, 3(2).

World Trade Organization (WTO) (2013). E-Commerce in Developing Countries: Opportunities and Challenges for SMEs, https://www.wto.org/english/res_e/booksp_e/ecom_brochure_e.pdf, (2016/03/10)
Yasin, S., Haseeb, K. and Qureshi, R. J. (2012). Cryptography based e-commerce security: a review. International Journal of Computer Science Issues, 9(2), 132-137.