Risk Management in Online Transactions: An Issue of System and Network Security

Bushra Elamin
Prince Sattam bin Abdulaziz University

Available online at: https://ijact.in

Date of Submission	06/09/2019
Date of Acceptance	08/10/2019
Date of Publication	31/10/2019
Page numbers	3448-3452(5 Pages)

Cite This Paper: Bushra M.E. Elnaim. Risk Management in Online Transactions: An Issue of System and Network Security, 8(10), COMPUSOFT, An International Journal of Advanced Computer Technology. PP. 3448-3452.

ISSN:2320-0790

COMPUSOFT
An International Journal of Advanced Computer Technology

RISK MANAGEMENT IN ONLINE TRANSACTIONS: AN ISSUE OF SYSTEM AND NETWORK SECURITY

Bushra Mohamed Elamin Elnaim
Department of Computer Science & Information, College of Science and Humanities in Al-Sulail, Prince Sattam bin Abdulaziz University, Saudi Arabia

Abstract: The following research paper is focusing on the research of online retailing adoption while challenges that are being faced in the area of system and network security. The research explores the major issues that put noticeable influence on the decision of customers who prefer to shop from the online retailers in Saudi Arabia as well as provide the clearer perspective for the online retailers to deal with the current situation of security. The advent of e-commerce has provided various opportunities to grow the business. E-commerce business is said to be incomplete if there is no significant payment gateway. However, despite having a feasible option of cash, people are mostly worried about the after-effects that pose serious threats for the same. Today, there are too many reports of data breaches, phishing attacks, website spoofing, payment card skimming (credit /debit cards), fraud in online transactions, malware attack (malicious code attack of viruses, worms, Trojans, and bots), hacker/cracker infiltration, vandalism, and identity theft related to bank details or credit cards. Like any system development, security risk management is an integral aspect of online transaction gateways. This research work explains how online transactions have become a bane rather than a blessing because of the threats posed upon it. It further defines the customer's perception as the qualitative research while providing better insights that how consumers look upon these issues and how they expect the improvements in e-commerce since it is certainly an advanced approach of a business.

Keywords: Saudi Arabia and e-commerce, ecommerce growth, online business, security threats, cyber threats in e-commerce, transactional insecurities, network and information security, e-commerce transactions.

I. INTRODUCTION

Saudi Arabia is remarkably adopting technical developments just like the other developed countries whereas online shopping is also being common there. However, there are still some major concerns that remain in regard to information technology and its security. The concept of IT risk management is regarded as a system of a wider enterprise related to risk management. Previously, the information systems of the organizations have seen the rise of security breaches. The current era of the e-commerce web application is faced with the vulnerabilities, manipulated by hackers and other people possessing negative vibes and emotions. These days' online frauds are most common and are on the rise than ever before (Sreedhar, 2018).

The idea of this research is to determine the troubles and insecurities in regard to transactions in a case when consumers deal with online retailers in Saudi Arabia. The main objectives of the research include understanding of the transactional insecurities, determining the influence of the network insecurities on e-commerce and knowing the perspective of users about online shopping and the threats they face in online shopping. This research will give the deep insight of the facts that why cyber threats are also the threat on county's economical development.

II. Material and methods

In the year of 2016, according to World Bank Group, Saudi Arabia was determined as of the top ranking easy doing business country. However, in recent years, that ranking has dropped by on a noticeable rate. There are different significant factors that researches found out on this fall while one of them was a complicated procedure of registering the business [1]. It takes a lot of time and numbers of processes in order to start a business in Saudi Arabia and this difficulty led to the other difficulties onwards. The complication in starting up with the e-commerce businesses due to the absence of regulations and particular standards for business makes is further difficult for consumers to find the reliable online services as well as security in making online transactions for shopping. The public certainly wants to utilize e-commerce services on a global level while on the other side entrepreneurs also need to utilize this opportunity but it is not possible unless brands grab the trust of consumers while network and information security make considerable improvement in this area. There are numbers of benefits of e-commerce that can be enlisted while some of the recent studies adverts that a lot of countries are utilizing the source of the internet while specifically in Saudi Arabia, the progress of spreading e-commerce is not that fast than the others. According to statistics, almost 8% of the population in Saudi Arabia use online stores for shopping while only 6% uses the online banking services and only 7% of the population uses the internet to make online reservations [7]. According to the world perspective, it is an extremely low figure, however, in comparison to the other middle-east countries Saudi Arabian e-market is ranked as the second large market which almost makes $520 from the online selling in the year of 2011. Slowly and gradually the successful e-commerce market is evolving the region of Saudi Arabia while people are starting to utilize the online payment methods at a little improved rate [3]. Online payments are certainly never completely safe but it largely depends upon the network and information security [2]. The variety of gateways of transactions is already present however consumers are usually confused about what to trust and what to now. These insecurities have the roots from a background which eventually affected the rate acceptance of digital usage in sensitive matters like transactions.

For the matter of fact consumers, as well as online merchants, expect that online selling and buying is safe, easy, and efficient. However, the involvement of payment processors and banks complexes the situation related to e-Commerce transactions. Additionally, the advancement of technology in e-wallets and the smart phones have to lead to competition among PSP to increase and maintain their share in the market [6].

There cannot be anything more precious than the information of the customer, and it is also a very sensitive issue that may spark a whole new controversy. It is the responsibility of the online shopping/ banking service to secure the personal information that a customer provides. The details should remain between the customer and online service. These include various contingents such as an address, name, age, date of birth, and sex. Further information that should remain confidential includes sexual lifestyle, ethnicity, political opinions, religious or philosophical beliefs, or health must also be treated as confidential [2]. Besides those other aspects that should be private includes incoming or outgoing personal correspondence, current contact details of family, guardian, etc. bank details, medical records or history, issues related to personal care, service records and file progress notes, individual personal plans, assessments or reports, and guardianship orders. The customers who are adults can indicate which information provided by them is to be treated as confidential or personal [3].

As far as credit card transactions are concerned in e-commerce portals, people tend to prefer those platforms which are authenticated. Its process comprises of the authenticity of the card as well as the identity of the card-holder. In order to reduce charge-backs and fraudulent transactions, the Credit Card Associations of Visa and MasterCard have introduced various services related to authentication. In order to verify the information of the transaction, especially in a card-not-present environment, is a topic we write about often, and for a good reason. The fraud of a credit card is a common thing in today's day and age. Many of the merchants are unfamiliar with the methodology of transaction verification. Presently there is no such way to introduce which provides protection against the scenarios of fraudulent attacks. Various other best practices and tools for fraud prevention can also be considered for the purpose of implementation such as fraud screening procedures, maintaining negative files, and using velocity limits and controls, etc.

Mobile apps are increasingly in demand and used by many consumers for the purpose of online transactions [5]. However, there are numerous complex code vulnerabilities, malware, unsafe app capabilities, and hidden processes included in it. The conditions continue to worsen in case of regular updates. The best way to deal with such issues is through Layer 7 assessment, real-time mobile application penetration, testing for malware detection, and log analysis as well as many others.

The process of mobile payment is a complex one, due to which many security issues arise. Many transaction systems include various parties in between the consumer and the merchant such as the payment card network, acquirer, and the card issuer, as well as others. Thus, it is easier for the criminal minded individuals and groups to intervene in between and take the fullest advantage of the loopholes in between [6]. The biggest issue many mobile users have is that they have absolutely no idea how and where their data is used. Some time back, one of the most popular mobile app payment aficionados stored information that was accessible easily. However, the issue was quickly resolved, once it arose, but for the app creators, a lesson was there to be learned. Luckily nothing went wrong or otherwise, this would have lead to a total disaster [4].

Fig. 1 Payment methods according to time

Furthermore, there is non-repudiation which refers to as an assurance that a person cannot deny, it is the communication between the two parties who mutually agree. As far as online transactions are concerned, digital signatures are required as the simplest way to obtain non-repudiation [4]. The digital signature once created, bounds the person so that he cannot deny later. However, experts warn that there is no guarantee and therefore suggest that multiple approaches should be implemented including unique biometric information capturing.

III. Experimental Work and Analysis

The consumers and the merchants have their own reasons to be uncomfortable with e-commerce platforms whereas some of the interviews and questionnaires helped the study to know the perspective of the consumers about e-commerce. These quaternary include:

1) What are the major factors that do not let consumers trust or utilize e-shops in Saudi Arabia and the responses include:

- Unavailability of the physical inspections
- Transactional insecurities
- Complicated methods of payment
- Fear of Internet threats

2) Another question for knowing how e-commerce can be promoted in Saudi Arabia and the responses include:

- *Providing guarantees*
- Assuring secure transactions and billing processes
- E-stores must be in government's supervision
- Provide good quality products and reasonable pricing

B. What is the typical Payment Process that is being utilized?

As per typical approach, most of the online stores use the method of carts for processing payment process. Once the customer is finished shopping, one is supposed to provide card details so that, information can be sent back to the bank and retailers can proceed with further payment processes [3]. Banks perform their own authentication processing in order to know if an authentic person is performing transactions and send approval. If there is an authentication issue, the request would be denied and the customer will get the notification however if it is accepted, the retailer can proceed with the shipping procedure. Typically, there is also the login procedure which is required for the user to make online orders. This data is used for identifying the user in order to avoid the billing frauds. However many of the retailers have skipped this process since they take a lot of time and many customers do not feel comfortable to provide information to the online retailers. It does provide significant flexibility to the users but at this point, insecurities of the consumers rise [4]. Though it lessens the rate of shopping cart abandonment and allows consumers to shop as a guest it raises the rate of uncertainty. However, it is also useful from some of the security perspective since consumers' sensitive information like address and credit card details will not be on the online platform and this will help to reduce the risks of transaction frauds and hacking threats.

C. Security Threats in E-commerce Systems

The scenarios of risk occur when the events if threats impact the system of e-commerce. The classification of threats is another area that plays a vital role in information security [8]. There are threat techniques and threat agent. The initiative of the security threat is usually taken by the threat agents. They exploit one's system vulnerabilities and attack on the system's assets. The current attack that came into notice is much similar to the attacks that are being detected n the web applications. There are numbers of attack patterns that have been already discovered in the area of e-commerce and in order to make the risk management better, awareness about these patterns is compulsory for the online retailers in order to make their business secure for themselves as well as the consumers [9].

D. Security Impact of Threats on E-commerce Systems

The security is the key factor of any business and as far as e-business is concerned, it is a compulsory need for it. Along with the technical development, threats are becoming strong every day and handling them is becoming tough as well. In that case, the countries in middle-east do suffer in order to provide a security guarantee to its people. There can be different consequences of the threat which can be defined as the impact of threats on the system while the risks can be diverse. Specifically about the transaction insecurity, the data of consumers can be leaked while also can be utilized to make illegal transactions. These issues were not that prominent few years back while the countries that are well-known for their technical development have been the target of attackers lately [7]. There are numbers of events recorded related to cybercrimes while lack of network and transaction security led these events to get worse. In order to make an online business work, consumers trust is essential but different regions are lacking in providing quality security which is eventually being the part of their failure in making e-commerce common in the region. Ultimately, the impact of these threats on consumers results in fear and uncertainty about their information security.

IV. Results and Discussion

Therefore, Saudi Arabia may have been improving in the terms of e-commerce as compared to the other countries of middle-east but it still needs to work on the area of network and transaction securities in order to gain the trust of consumers and assure them that their information and money is secure. There are some significant factors that must be utilized in order to make the security better of e-commerce that is being discussed as follow:

a) Educate and train your staff on e-commerce risk:

The degree of your hazard presentation to a great extent relies upon your business arrangements, operational practices, the extortion recognition and aversion devices you have actualized, security controls, and the sorts of items and administrations that you give. Everybody in your association ought to comprehend the dangers related to online exchanges and have the capacity to pursue your built up hazard the executives' methodology.

b) Find the right payment processor:

The correct charge card handling organization will give successful hazard the board backing and help you comprehend the particular web-based business extortion hazard and obligation. Sufficient client information assurance capacities are additionally something you will need to think about when making your determination.

c) Create essential website content:

Your site must incorporate and noticeably show your security, transporting, return and discount approaches. It must be dependable and to give clients a simple and straightforward route. Setting connects to these arrangements in the footer of your site will make them present on each page.

d) Focus on risk reduction:

An all-around structured deals request procedure will enable you to address various hazard concerns. You ought to show or feature required exchange fields in your online installment acknowledgment structure and confirm card and cardholder data that you get from your clients over the web.

e) Develop internal fraud prevention structure:

The benefit of your organization of e-commerce relies upon your interior systems and controls for limiting misrepresentation. A hazard the executive's structure joined with satisfactory exchange controls, will enable you to keep away from extortion related misfortunes.

f) Use fraud prevention tools:

There are various tools used for fraud prevention to help decrease your hazard introduction. The most generally utilized among them are the Address Verification Service (AVS), the Card Security Codes (CVV2, CVC 2 and CID), Verified by Visa and MasterCard SecureCode.

g) Build a fraud screening process:

At the point when enough actualized, the screening of online card exchanges can enable you to limit misrepresentation for huge ticket things and for high-chance exchanges.

h) Protect your merchant account from intrusion:

Actualizing proactive measures can limit the danger of hoodlums accessing your shopping basket or installment passage and making false reserve stores.

i) Participate in Verified by SecureCode of MasterCard and Visa:

The two extortion anticipation instruments improve security by expecting cardholders to verify themselves by entering a secret key amid the checkout. The secret word is checked by the card guarantor and, if right, the exchange is permitted to be finished. Executing Verified by Visa and MasterCard SecureCode shields vendors from extortion related chargebacks.

j) Secure The Process Of Routing Your Authorizations:

You should guarantee that your approval demands are submitted in a safe and productive way before you can begin tolerating card installments once again the web.

k) Establish a Process for Handling Transaction Post-Authorizations:

You have to set up a powerful procedure for managing affirmed and declined approvals before satisfying a request.

l) Ensure PCI compliance:

The Payment Card Industry (PCI) Data Security Standards (DSS) furnish online shippers with norms, methodology, and devices for ensuring touchy record data. You will require solid encryption capacities for information transmission and compelling inward controls for ensuring put away the card and cardholder data. You will likewise need to survey your safety efforts all the time.

V. Conclusion

Thus, for the shopping arenas and the business organizations, the most important thing is to gain the attention of the customer is to have a secure transaction mechanism. Providing a suitable product online is just not enough when they are unable to provide security to the transactions online. Saudi Arabia is lacking in improving the e-commerce rate from different countries because of their major focus lack from providing complete network and transaction securities to its consumers. Most companies make use of the Secure Sockets Layer (SSL) protocol to gain the trust of the customer and make them believe that the website through which they are shopping is secure. Organizations not only perform transactions with other parties and customers but also for the purpose of advertisement. These are the initial steps to improve the quality of e-commerce in particular region while there are some other precautionary measures that need to be implied after these.

ACKNOWLEDGMENT

The author would like to thank College of Science and Humanities in Al-Sulail at Prince Sattam bin Abdulaziz University for the moral support that he found from this institution to complete this research.

REFERENCES

[1] Uma Sekaran, Roger Bougie.(2016) Research methods for business: A skill building approach. Seventh edition. Chichester, West Sussex, United Kingdom: John Wiley & Sons, [2016].

[2] Chaffey, D. (2015a) Digital business and e-commerce management: strategy, implementation and practice. Sixth edition. Harlow, England: Pearson.

[3] Cavusgil ST, Knight G, Riesenberger JR, Rammal HG, Rose EL. International business. 2nd edition. Melbourne, Vic: Pearson Australia, 2015. p.632.

[4] Eyad Makki, Lin-Ching Chang. (2015). Understanding the effects of social media and mobile usage on e-commerce: an exploratory study in Saudi Arabia. International management review.Vol 11, no 2, p.98.

[5] Layla Alsheikh, Jamil Bojei.(2014) Determinants affecting customer's intention to adopt mobile banking in Saudi Arabia. International Arab Journal of e-Technology. Vol 3, no 4. pp 210-9.

[6] E. Makki and L.-C. Chang, "E - Commerce in Saudi Arabia: Acceptance and Implementation Difficulties," in The 2014 International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government (EEE'14), 2014, pp. 114–120. Accessed from https://pdfs.semanticscholar.org/23ba/49517523d5edaf8307eb92da92d7b4c61352.pdf

[7] F. Aleid, S. Rogerson and B. Fairweather,(2010) "A consumers' perspective on E-commerce: practical solutions to encourage consumers' adoption of e-commerce in developing countries -A Saudi Arabian empirical study", International Conference on Advanced Management Science, Chengdu, China, vol. 2, pp. 373-377. Accessed from https://arxiv.org/ftp/arxiv/papers/1302/1302.0820.pdf

[8] Khalil Nahla (2014). Factors affecting the consumer's attitudes on online shopping in Saudi Arabia. International journal of scientific and research publications. Vol 4, No 11.pp. 1-8.

[9] E. Makki and L.-C. Chang (2015). E-commerce acceptance and implementation in saudi arabia: previous, current and future factors. International Journal of Management Research and Business Strategy. Vol 4, No 3. Pp 29-44.