IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 6, Ver. II (Nov – Dec. 2014), PP 18-22
www.iosrjournals.org

Effects of Cyber Security on Selected Mobile Phone Payment System in Nairobi Central Business District, Kenya

Constantine Matoke Nyamboga[1], Wekesa Nelson Barasa[2]
[1]*Department of IT, School of Pure and Applied Science, Mt. Kenya University, Kenya*
[2]*Associate Faculty, Faculty of Science and Technology, Kisii University, Kenya*

Abstract: *The study aimed at examining effects of cyber security on selected mobile phone payment systems in Nairobi County, Kenya. A purposive complete census was conducted to collect data from the selected mobile phone service providers; Safaricom. A cross-sectional survey research on the other hand was employed to a population comprising of; mobile phone users and mobile phone money merchants. To collect data, questionnaires and scheduled interviews were conducted. Content Validity Index was used to measure the relevance of the questions in relation to the variables under study. Also, reliability test was conducted to determine the consistency of the scales used to measure the study variables. Once data had been collected, it was cleaned, coded and stored as a database of statistics and analysed using descriptive statistics such as frequency distributions, weighted averages, and descriptive variables, correlations and linear regression models. From the findings, it was observed that there is a lack of sufficient awareness education and information on the use and existence of mobile phone money services, those who know about it majorly use it as a money transfer service (sending and receiving money) from one mobile phone user to another. Only a few respondents use the service to effect core business transactions (paying bills and buying of goods and service).*
Keywords: *Mobile money; cyber security; mobile phone; mobile money service*

I. Introduction

In today's world of information communication and technology (ICT) and related technologies being used in almost every aspect of our lives, people are left with no other choice but to adopt the change. Technology has not only revolutionized people's lives but also business operations. Through electronic commerce, the process of buying and selling or exchanging of products, services and information via computer networks including the Internet are effected [1]. These current trends and demands have resulted to financial institutions banks and micro finance institutions such as Barclays, Kenya Commercial Bank, Equity etc. to produce and also encourage their customers to use electronic money. Mobile phone service providers have also joined the bandwagon and developed platforms to facilitate the use of electronic money-mobile money payment systems.

The Kenyan government through the Communication Commission of Kenya (CCK) has recently signed an agreement with International Telecommunications Union to boost cyber security in the country and more so in relation to electronic money [2]. "Cyber insecurity affects everyone from national governments, the public sector, the private sector, and ordinary citizens in a country"[3]. The availability of affordable mobile phones in the market and mobile phone network coverage extending even to remote areas of the country and having acceptable mobile money payment systems, mobile commerce is totally revolutionizing Kenya. The mobile phone has become a common device and almost every Kenyan own one. The mobile phone has become the platform of choice for running electronic commerce applications. It is for this reason that the mobile phone accounts for a huge number of devices that make up the cyberspace compared to computers and other related devices. With the rapid growth and penetration of mobile phones and specifically mobile commerce, most business establishments and institutions are slowly adopting it however with reservations.

The main of this study was to investigate the effects of cyber security on selected mobile phone payment systems in Nairobi CBD as well as to identify challenges and suggest possible solutions. Other objectives of the research include to; establish the scope of mobile phone payment systems in Nairobi Central Business District; determine security measures put in place for mobile phone payment systems in Nairobi Central Business District, and to investigate the challenges being faced in instituting cyber security measures in Nairobi Central Business District.

II. Literature Review

Electronic commerce provides the capability of buying and selling products, information and services on the Internet and other online environments-cyber environment [4]. As for any trading activity, the issue of safe and reliable money exchange between transacting parties is essential. In an electronic commerce environment, payments take the form of money exchange in an electronic form, and are therefore called

electronic payments. E-payments are an integral part of electronic commerce and are one of its most critical aspects. Electronic Payment Systems (EPSs) are summoned to facilitate the most important action after the customer's decision to pay for a product or service and to be able to deliver payments from customers to vendors in a most effective, efficient and problem-free way. The role of electronic payment systems is pivotal for the future of electronic commerce, whose further growth depends on the timely development of EPSs.

The principal objective of cyber security is to ensure the 'attainment and maintenance of security properties of the organization and user's assets against relevant security risks in the cyber environment'. There are various types of breaches that compromise security for example virus, unauthorized access, theft of proprietary information, denial of service, sabotage, web site defacement, etc. Although these security incidents are continuously rising, organizations have come to be aware of the importance of information security. Assessing the impact of security breaches is very difficult because costs of security breaches are not very ease to quantify [5]. All over the world, there have been reported news and surveys being conducted on the magnitude of the monetary losses from the ever increasing breached incidents

With the rapid growth and evolution of ICT as well as Internet penetration in Kenya, government, financial and educational institutions are now relying more on the internet as an infrastructure to deliver on their core business. This reliance on the Internet infrastructure for basic operations such as trade, education, and health makes cyber security a matter of concern for the Republic of Kenya. The Ministry of Information and Communication (MoIC) is working closely with the Central Bank of Kenya (CBK), Kenya Police and the Communication Commission of Kenya (CCK), has ensured that cybercrimes which are becoming a common occurrence in the country are eliminated and also that systems are not abused [6].

Since the inception of mobile phone money in Kenya, it has continued to surpass other forms of EPS. Mobile phone money and payments can be used in the following dimensions of electronic commerce, Business to Business (B2B), Business to Consumer (B2C) as well as Government to Business (G2B). From the previous CBK statistics, mobile phone money accounts for the large volumes of transactions. Mobile phone money can be used for varied functions example, mobile phone money transfer, payments of goods and services, settling of bills/invoices etc. Mobile phone money has also been used in payment for digital content e.g. ring tones, logos, news, music, or games. Payments for physical goods are also possible, both at the vending and ticketing machines, and at manned Point-of-Sale terminal [7]. Mobile phone money in Kenya initially was developed to facilitate the transfer of cash from urban to rural areas linking and building into family and social ties.

It has been argued that for widespread use and customer acceptance of mobile phone payment services, both perceived and technical levels of security should be high [8]. For customers, privacy should not be compromised and there should be no possibility of financial losses. For businesses, customer authentication is important. According to [9] "a secure mobile phone payment scheme provided by secure hardware within a trusted mobile phone payment system should detect any malicious modifications and intrusions of a payment application and/or the corresponding data during their life cycle". It is therefore that for any secure messaging system, confidentiality, integrity, non-repudiation and authentication should be guaranteed.

III. Research Methodology

The research was conducted using the cross sectional survey design where a selected representative sample was interviewed and/or asked to respond to well-structured questionnaires and interview schedules. This research design was suitable for the collection of data from several respondents at one point [10].

The research study was conducted on a selected mobile phone money service in Nairobi Central Business District (CBD). The population for the research was the dominant mobile phone service provider; Safaricom, Safaricom mobile phone subscribers, and Safaricom M-PESA money agents/merchants. The Nairobi CBD comprises of 352 M-PESA agents and/or merchants [11] and approximately 3,138,369 people [12] most of whom are mobile phone users both M-PESA agents and M-PESA subscribers.

A purposive sampling procedure was used to collect data from the mobile phone service providers and 10 is the number of respondents sampled from the company. A proportionate stratified random sampling technique was in turn employed in the CBD to seek responses from mobile phone users and mobile phone money merchants. According to Yamane Taro's study (as cited in [13], the sample size was calculated using the following formula;

$$n = \frac{N}{1 + N(e)^2}$$

Where;

n is the sample size,
N is the population (approximately 3,138,369) and
e is the level of precision,90% confidence level.

The following was then derived,

$$n = \frac{3{,}138{,}369}{1 + 3{,}138{,}369(0.1)^2}$$
$$n = 99.99681$$

The study used a 90% confidence level, which meant that if the same population was sampled later again same estimates could be made, and the results would represent true population parameter of 90% of the cases. The research study applied two types of instruments to collect data from the mobile phone subscriber and mobile phone money agent or merchant. Interviews were employed when it came to interrogation of the technical staff of the mobile service provider; Safaricom as primary data and secondary data from journals, magazines, books as well as published and unpublished research works.

An expert (supervisor) was consulted to scrutinize the relevance of the questionnaire items against the objectives of the study and there was a strong signal of them being relevant to the study. Besides, the instruments were checked to ensure they produced accurate and credible results. Reliability test were conducted to determine the consistency of the scales used to measure the study variables. The instruments were designed with main focus being on content where the information collected from the respondents would provide stable ground for analysis and portray a true picture; that the information was merely a representation of the entire population.

The data collected was cleaned, coded and stored as a database of statistics and analysed using descriptive statistics for example, frequency distributions, weighted averages, and descriptive variables, correlations and linear regression models

IV. Results and Discussions

From the respondents, Eighty four (84) percent of respondents were found to have reliable data to be used in the research from the mobile phone subscriber's sample. Seventy eight (78) percent of respondents on the other hand provided reliable data from mobile phone merchants and agents. From the Mobile phone subscribers, nineteen point five (19.05) percent from the sample were to be possession and also have used mobile phones below two year, Forty seven point six two (47.62) percent indicate that they are in possession and have used mobile phones between 2 years and 5 years, thirty three point three, three (33.33) percent on the other hand have had and used it in the last 5 years. In relation to mobile phone merchants, sixty nine point (69.23) percent indicated that they are in possession and have used mobile phones between 2 years and 5 years. Thirty point seven, seven (30.77) indicated that they are in possession and have used mobile phone for over 5 years. From these responses, it is can be observed that a hundred (100) percent are in possession and have used a mobile phone within the last five years.

In relation to the frequency of usage, ninety two point nine (92.9) percent reported to using the service more for sending money, eighty eight point one (88.1) percent reported to be using the service for receiving money while forty two point eight (42.8) percent reported to be using the service for paying bills. From these statistics, it is important to note that despite Safaricom mobile money service being too popular, most of the respondents use it majorly as a money transfer service (sending and receiving money)

When it comes to using the service for buying goods and services, the study indicated that sixteen point seven (16.7) percent use the service very frequently, nineteen (19) percent use the service frequently, nine point five (9.5) percent use the service occasionally to buy goods and service from shops or markets. Thirty three point three (33.3) percent of the respondents reported that they rarely use it, while eleven point nine (11.9) percent on the other hand said that they have never used the service at all for buying goods and services. This response is strange but the main reason is that the service is not acceptable by merchants and mobile phone users themselves would prefer to use other means despite having money in their mobile phone money service. It is important to note that, from the findings of this study also, the mobile service provider reports that it's trying to inform and educate the population in relation to the subscription, use and conduct when using the service and that is has been evaluated as follows; ninety two point nine (92.9) percent reported that the felt the information being provided by the mobile provider is effective and would result to the population being more aware and informed on the usage, security and conduct while using mobile phone money service.

Table 4.1, represents mobile phone users and its evident that independent variables were not significant ($p>0.05$), these were cyber security (0.092), and accessibility levels (0.485). However, this did not affect the usage while effectiveness of information provided by the service provider (0.037) and CCK regulation (0.001) are significant ($p<0.05$).

Table 4.2, represents the regression coefficient for the mobile phone merchants and it implies that the variables being studied namely; providers' effort to encourage subscription and usage, frequency of usage, cyber security effects and merchants opinion on the service have no effects on the reasons by which mobile phone merchants have chosen to use the service and that they have no direct influence of the extent to which users utilize the mobile payment systems.

Table 4.1: Regression Coefficient for Mobile Phone Users

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	16.253	2.272		7.153	.000
	Cyber Security	-.731	.367	-.304	-1.990	.054
2	(Constant)	11.904	3.101		3.839	.000
	Cyber Security	-.530	.369	-.220	-1.437	.159
	Effectiveness	.675	.341	.303	1.983	.055
3	(Constant)	7.433	2.979		2.495	.017
	Cyber Security	-.521	.322	-.217	-1.621	.114
	Effectiveness	.685	.297	.308	2.304	.027
	CCK Regulation	.838	.234	.461	3.589	.001
4	(Constant)	5.926	3.681		1.610	.116
	Cyber Security	-.576	.333	-.239	-1.729	.092
	Effectiveness	.656	.302	.295	2.170	.037
	CCK Regulation	.903	.252	.496	3.580	.001
	Level of Accessibility	.214	.303	.101	.706	.485

a. Dependent Variable: Usage

Table 4.2: Regression Coefficient for Mobile Phone Merchant

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	9.704	1.683		5.764	.000
	Providers effort	-.259	.357	-.119	-.726	.472
2	(Constant)	8.806	2.414		3.647	.001
	Providers effort	-.331	.386	-.151	-.858	.396
	Frequency usage	.073	.140	.092	.523	.604
3	(Constant)	12.312	14.062		.875	.387
	Providers effort	-.594	1.110	-.272	-.535	.596
	Frequency usage	.062	.149	.078	.419	.678
	Cyber Security effects	-.284	1.123	-.133	-.253	.802
4	(Constant)	9.697	14.971		.648	.522
	Providers effort	-.435	1.157	-.199	-.376	.709
	Frequency usage	.047	.152	.060	.310	.758
	Cyber Security effects	-.168	1.154	-.078	-.145	.885
	Opinion	.111	.201	.099	.553	.584

a. Dependent Variable: Reasons

Finally, from the mobile service provider's point of view, fraud, lack of acceptability, network coverage and number of agents/merchants affect the adoption and usage of mobile service provider and as such they have been identified and are being tackled. The respondents also indicated that the role being played by the CCK is in the regulation and provision of information in relation to mobile phone money service is satisfying and encouraging the users to use the service.

The Communication Commission of Kenya (CCK) was rated in relation to the process of educating and promoting the use of mobile phone money services. The respondents indicated that

1. Forty two point nine (42.90) percent stated that CCK is fairly involved in educating the public on mobile phone money usage
2. Forty five point two (45.2) percent mentioned that the CCK is highly involved in establishing guidelines on how to use mobile phones and mobile phone money
3. On the other hand forty seven point six (47.6) percent said that the CCK is highly involved in the formulation and laying down of policies to ensure secure mobile money services are provided.

From the study, it became clear that for mobile phone money service, more so, the mobile phone payment system for it to be widely accepted and used all over as an alternative means of payment several issues have to be solved. First and foremost, there should be both public and private education and information flow in relation to the awareness of its existence, how to use it as well as how to protect it and themselves from being targets of cybercrime. Secondly, the mobile networks have to increase the number of agents or merchant as

some people would like to use the service but are unable due to its unavailability. Again, the mobile providers should spread widely and ensure that their network is available and reliable all the time. Thirdly, the mobile phone users should be open and be encouraged to embrace these systems as they are already here with us and provide us with a convenient method of conducting business transaction and operations faster, easier and safer than carrying cash.

V. Conclusion and Recommendation

From the study analysis, the following conclusions are made;

1. There is high number of mobile phone users in the country and that number is set to increase in the coming years.
2. Mobile phone money services are here and cannot be wished away therefore both users and merchants have to accept, adopt and use it as an alternative method of effecting payments
3. The use of mobile phone money services is encouraging but at the moment it is mostly used for transferring money (sending and receiving) from one location to another
4. The CCK regulation is most critical factor influencing the level of usability on the mobile phone payment system, followed by effectiveness of the by the service provider in relation to mobile phone money usage, thirdly, cyber security and lastly the level of accessing mobile phone payment service.
5. The merchant/agents has little influence on the usage of mobile phone money service because they rely on the service provider in the provision of their services therefore, effectiveness, cyber security, level of access and CCK regulation are beyond their bound

From the study, it became clear that for mobile phone money service, more so, the mobile phone payment system for it to be widely accepted and used all over as an alternative means of payment several issues have to be solved. First and foremost, there should be both public and private education and information flow in relation to the awareness of its existence, how to use it as well as how to protect it and themselves from being targets of cybercrime. Secondly, the mobile networks have to increase the number of agents or merchant as some people would like to use the service but are unable due to its unavailability. Again, the mobile providers should spread widely and ensure that their network is available and reliable all the time. Thirdly, the mobile phone users should be open and be encouraged to embrace these systems as they are already here with us and provide us with a convenient method of conducting business transaction and operations faster, easier and safer than carrying cash.

This study was limited to finding out the effects of cyber security on mobile phone payment systems in Nairobi CBD, case of Safaricom Limited. It was therefore not comprehensive and is open for further research on the following recommended areas for comparisons, validity and reliability;

1. Other factors that affect mobile phone payments systems e.g. Technology, competition, politics, economy, globalization etc.
2. The longitudinal effects of cyber security on selected mobile phone money payment systems

References

[1]. Turban, E., Lee, J., King, D., & Chung, H. M. (2004). Electronic Commerce: A Managerial Perspective. (2nd ed.). Singapore: Addison Wesley Longman.

[2]. Nduati, L. (2012, April 3). Mobile money transactions to be audited by banks regulator. The Daily Nation. Retrieved April 3, 2012, from http://www.nation.co.ke/business/news/Mobile+money+transactions+to+be+audited+by+banks+regulator+/-/1006/1378798/-/5km5tc/-/index.html

[3]. Tamanikaiwaimaro, S. (2010). Cyber Security in the Republic of Fiji. Presented at the Internet Governance Forum, Diplo Foundation. Retrieved from http://www.diplomacy.edu/resources/general/cyber security-republic-fiji

[4]. Abrazhevich, D. (2004). Electronic Payment Systems: a User Centered Perspective and Interaction Design. Universiteitsdrukkerij Technische Universiteit, Eindhoven, Netherlands.

[5]. Ko, M., & Dorantes, C. (2006). The Impact of Information Security Breaches On Financial Performance of the Breached Firms: An Empirical Investigation. Journal of Information Technology Management, 7(2), 13–22.

[6]. Obura, F. (2012, April 2). CBK moves to secure mobile money transfers from hackers. The Standard Newspaper. Retrieved April 4, 2012, from http://www.standardmedia.co.ke/InsidePage.php?id=2000055455&cid=14&j=&m=&d=

[7]. Dahlberg, T., Mallat, N., Ondrus, J., & Zmijewska, A. (2006). Mobile Payment Market and Research - Past, Present and Future. Netherlands, 7(2), 165–181.

[8]. Carr, M. (2007). Mobile Payment Systems and Services: An Introduction. IDRDT Hyderarbad: IDRDT. Retrieved from http://www.idrbt.ac.in/respub_06.html

[9]. Li, Q., Zhang, X., Seifert, J.-P., & Zhong, H. (2008). Secure Mobile Payment via Trusted Computing. In IEEE Computer Society. Presented at the Third Asia-Pacific Trusted Infrastructure Technologies Conference. doi:10.1109

[10]. Kothari, C. (2010). Research Methodology, Methods and Techniques (2nd ed.). New Age International Publishers.

[11]. Safaricom. 2012b). Safaricom MPESA Agents. Safaricom. Retrieved March 28, 2012, from http://www.safaricom.co.ke

[12]. Ministry of State Planning, National Development and Vision 2030. (2010). Population Census 2009. Ministry of Planning. Retrieved April 11, 2012, from http://www.planning.go.ke/archive/index.php?option=com_docman&task=cat_view&gid=52&Itemid=69

[13]. Israel, G. D. (2012). Determining Sample Size. Program Evaluation and Organizational Development,Institute of Food and Agricultural Sciences(IFAS), University of Florida, Gainesville, FL 32611, 6, 2.