International Journal of Computer Science and Business Informatics

IJCSBI.ORG

Cyber Crimes Incidents in Financial Institutions of Tanzania

Edison Wazoel Lubua (PhD)
Mzumbe University, Dar Es Salaam Campus College

Abstract
This paper investigates the trend of cyber-crimes in Tanzania. The purpose is to evaluate challenges associated with cyber-crimes in mobile money services. The study acknowledges the provision of mobile money services by both telecommunication companies and local banks, the fact which poses a threat in the old fashion of addressing crimes. Data were collected from the Foreigscic Section of the Tanzania Police Force and users of the mobile-money services. The analysis used both descriptive techniques and the Pearson Correlation model to establish different facts. The conclusion is based on observed evidence, and it is placed in the last section of the paper.

Keywords: Cyber-crimes, cyber security, cyber laws, mobile money

Background of the Study
The use of the internet and other Information and Communication Tools (ICTs) transforms the way our societies perform their day to day activities. As the result of the importance of such uses in ICTs, the number of users is increasing in a daily manner. In 2011, about 7 billion people were connected to the internet (through computers and mobile phones) across the globe (KPM international, 2011). In Tanzania, about 7,500,000 users were reported in 2012, this is about 17% of the whole population (IPP Media, 2014). The number of people subscribed to the use of internet facilities, is the reflection of many activities completed through this platform. Therefore, the internet has transformed the way people perform different activities in modern communities.

Although a large group of people use the internet for different activities, a significant per cent of users do not use the facility for shopping purposes (Zickuhr, 2012)). In the United Kingdom, about 1/3 of internet subscribers are not shopping online due to fear of online security. Cyber-crimes reduce the confidence of consumers about the level of online security facilitated by service providers (Digital Policy Alliance, 2013).

A study about cyber security showed that the fear of cyber crimes cost the world community a large amount of money in establishing security protocols. In 2008 the

worldwide cost of cybercrime was approximately USD 8 billion (Intersecurity Magazine, 2013). Some of the recently characterized cyber crimes include corporate cyber espionage, stealing of intellectual properties, financial scams, computer hacking, downloading pornographic material from the internet, virus attacks, e-mail stalking and creating websites that promote racial hatred (Singer & Friedman, 2014).

Many countries face difficulties in addressing issues arising from cyber crimes, because they lack a concrete definition of computer crimes and how such crimes differ from traditional crimes (Aslan, 2006; Mayunga, 2013). Aslam (2006) defined computer crimes as a violation of criminal laws that involves the knowledge of computer technology for its penetration, investigation, or prosecution. Unfortunately, Africa has become the target of cyber crimes than the rest of the world where more internet users are victimized by these crimes than before. It is estimated that 80 percent of the computers in Africa are already infected with viruses and other malicious software (Kumar, 2010). The noted level of infection increases the level of vulnerability to cyber crimes in the region (Pack, 2013).

In the Tanzanian context, a significant percent of the population is connected to the internet (Lubua E. , 2014; IPP Media, 2014). As the result the government established a unit within the Police Force to address challenges of cyber crimes. However, the impact of cyber crimes is still threatening the security of internet users. In 2012, about 620 cases were reported to the cybercrime unit (Mayunga, 2013). The most reported crime was online stealing of money. Other reported crimes include obscene communications, computer forgery and life threatening messages.

It is evident that the increase of cyber crimes affects transactions which are conducted online in the Tanzanian community. Nevertheless a number of controls are introduced to address the challenge. Such controls include the use of authentication methods, the use of surveillance cameras and awareness campaigns about online safety. Some of the stakeholders are even proposing laws that allow online patrol by the Police Force. This paper discusses factors influencing the safety of mobile-money banking in the Tanzania context.

2. Statement of the Problem

The emerging ICT technology comes with a number of benefits to the community. In financial institutions (banks), clients are able to access different services without visiting bank premises. Nevertheless the use of ICTs for banking purposes comes with the risk of cyber-attacks. The failure to control the online activities provides people the room to conduct old crimes in a new way (Mayunga, 2013). Reports show that Tanzania lost approximately 892.18 billion through online crimes in 2012 (Mwananchi, 2012). Similarly, a number of studies conclude that the lack of cyber

crime laws creates a vacuum in the control of these crimes (IPP Media, 2014; Lubua E. , 2014; Pladna, 2008). Other contributing factors include the low technological literacy of users and technical security loopholes. In environments where the internet is lowly controlled, criminals conduct crimes anonymously (Paganinip, 2012). In Tanzania, the Chief of the Forensic Bureau suggests online patrol by Police officers as effective and efficient in addressing these crimes (Majaliwa, 2011); however, the international community is against this practice.

The government of Tanzania is currently implementing reforms aimed at addressing cyber crime incidents. Such reforms include the strengthening of the telecommunications regulatory body (through equipping it with modern technologies), raising the awareness of the law enforcing body and that of online-services users on cyber crimes. Despite these efforts, incidents of cyber crimes are still increasing. In this study, we determine:-

i.) Whether the rate of response from the mobile-money officers on queries from clients contributes to the level of security to clients.

ii.) Whether the nature of control of the Tanzanian mobile money platforms adequately address the challenge of cyber crimes.

3. Significance of the Study

This paper establishes the following:-

i.) It improves the knowledge of stakeholders about the adequacy of methods for addressing the challenge of cyber crime in Tanzania and other developing countries. The more important part is where it identifies employees of the mobile money companies and their clients as the most important part of stakeholders in addressing the challenge.

ii.) It shows the loopholes brought by the lack of the legislation to administer cyber issues in Tanzania.

4. Adopted Research Methods

The study used the Criminal Investigation Department of the Tanzania Police Force as the key source for secondary data about the trend of cyber crimes in Tanzania. Data were extracted from the cyber crime unit of the Police Force. This is the Police Force section where cyber crimes are reported. Moreover, the study interviewed employees and clients of the local mobile-money companies to understand their perception about the security level of the mobile money services.

Generally, the population of the study included employees of the Tanzania Police Force in the Department of Criminal Investigation (cyber crime unit). A sample included 50 respondents where 20 were Police Officers and 30 respondents were taken from employees of commercial banks in the online banking unit. Because

data were in two main groups, the study used convenience sampling to exploit data from respondents. The analytical model adopted is the Pearson Correlation Model. The study ensured that data were collected from original sources and were clearly audited for reliability reasons.

5. Cybercrimes in Tanzanian Financial Institutions

The use of ICT technologies in Tanzania is growing at a high rate. The rate of growth reported between 2000 and 2010 is about 450% (Lubua & Maharaj, 2012). It is further reported that about 45% of the Tanzanian population owns mobile phones (Genuchten, Haring, Kassel, & Yakubi, 2012). The increase in the use of the internet and mobile technologies has impacted the methods to which financial services are offered to clients. The majority of local banks offers their services through both traditional and online media. These banks have also incorporated the use of mobile phones in effecting financial transactions. Additionally, telecommunication companies do also offer financial services, which do not necessarily engage banks.

The use of mobile money services is in the upward trajectory in Tanzania. About 45% of the Tanzanian adults are reported to be using mobile money (Mayunga, 2013). A total of TZS 1.7 trillion was transacted through mobile money in 2012; this shows a significant shift of financial transaction from traditional options to the use of mobile money and internet (Ndulu, 2012). Unfortunately the increase of mobile money uses in financial transactions comes with new challenges. The most noted challenge is the impact of cyber crimes.

In 2012, about 627 cyber crime cases were reported. Figure 1 below shows the trend of cyber crimes as reported to the Foreigscic section of the Tanzanian Police Force. There is a steady increase of cyber crimes in Tanzania from 2009 to 2012. A simple explanation to the observed trend is that the increase of mobile uses for banking purposes do also increase the rate of crimes associated with mobile money. This is because more users of the mobile phones were subscribed in every year.

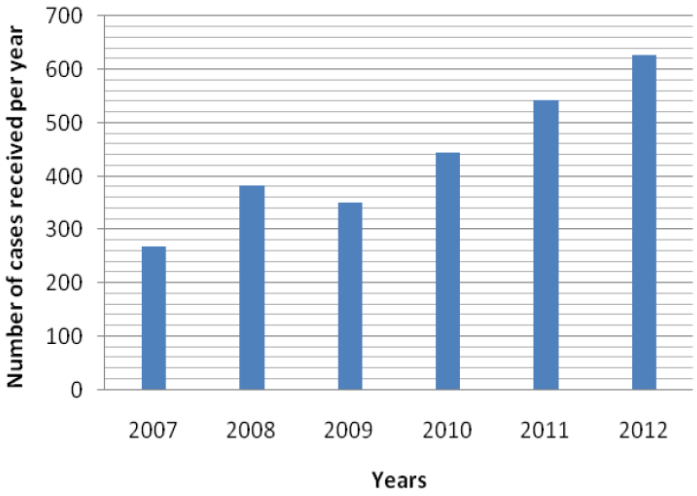

Figure 1: Cybercrimes trend
Source: (Tanzania Police Force, 2012)

The following are suggested by the literature to contribute to the increase of mobile money crimes: the lack of cybercrime policy, inadequate system security and low awareness of mobile money users (Mayunga, 2013). The results of the interview with the Cybercrime unit of the Tanzanian Police Force proposed that online patrol could address the challenge. Online patrol is the idea borrowed from the traditional way that the Police Force uses to combat crimes. However, this suggestion receives criticism from internet users across the world, since it allows the government to scrutinize internet information from users. Besides, the suggestion remains to be a theory rather than solution due to a number of unaddressed questions. One of the questions is the efficiency of online patrol since the traditional police patrol does not adequately address the challenges of crimes occurring in traditional societies.

While the security of online transactions remains as the primary concern of mobile-money providers and other stakeholders, the most suitable solution is that which does not intrude the privacy of users. Any proposed solution must balance the relationship between mobile money users, service providers and policy makers in ensuring online safety without intruding one's privacy.

5.1 Cyber Law

Tanzania adopted her first National ICT Policy in 2003. It aimed at increasing the pace for providing different services to the society through the use of ICT tools (Tanzania National ICT Policy, 2003). Since then, more people are using ICT tools in their routines; nevertheless, this increase results to the rise of a new form of crimes. The study by Mayunga (2013) emphasizes that the lack of cyber policy in

Tanzania contributes significantly to the increase of cyber crimes. In this study, we acknowledge improvements made by the legal system of Tanzania in addressing online cases where online evidences are now accepted. Initially, the Court System of Tanzania did not accept online evidences (Msuya, 2014).

It is the expectation of stakeholders that the instalment of the cyber law in Tanzania, would address a number of issues concerning the safety of the mobile-money users. First, the law would address the issue of privacy. The Tanzanian society is found under the socialistic and the self-reliance ideology where the concept of individualism had little importance (Nyerere, 1967). In addition, the majority of users of the mobile money formerly used traditional methods for making different transactions where privacy was not a serious concern. Currently, the lack of defined levels of privacy to users (of mobile-money), exposes them to threats of online theft. This is because online methods for accessing financial services require the storage of several individual information to the database of the company. The information may be used against the owner.

In certain incidents, the study witnessed the mobile money Kiosk operators who required their clients to submit the login credentials to receive assistance in accessing their money. Mobile money users happen to submit such information out of ignorance. It is possible that some of the Kiosk operators use such data against their clients, this results to the rise of online crimes. The interview found several clients of the mobile money services who admitted to have submitted such credentials without knowing the possible consequences. Moreover, about 30% of the surveyed sample admitted that someone who pretended to be an officer of the mobile-money operator once demanded the submission of login credential through email or SMS for some reasons including updating user's information. The combination of the socialistic life and the illiteracy level of members of the community threaten the safety of users who transact through mobile money.

Also, there is nothing that legally identifies who has to access the stored information of clients, what type of information can be accessed and when should that access be granted. The lack of guidance grants mobile money operators the unmonitored privilege to the access of clients' information. It is this loophole that the unfaithful employees use to access clients' information and money. The results from the survey support this observation since about 44% of the mobile money clients reported an incident where the loss of their money was contributed by the mobile money operator.

Based on observations above, the establishment of a comprehensive legal system that address issues associated with privacy would decrease challenges associated with

cyber crimes.

Secondly, the cyber law would decrease the potential for online abuse. In the absence of cyber laws, the unfaithful government leaders and business corporations use the captured data of clients according to their wish. In Tanzania, mobile subscribers and mobile money users are registered. The registration system stores the information about users and transactions that they make. Economically, knowing expenditures of a person lead to an easy prediction of the income, hence an easy access to the information poses security threats to consumers of mobile money services. A number of incidents were reported in the previous year about mobile money kiosk operators and their clients who were ambushed by robbers. It is most likely that the thieves were well informed of the cash flow of the mobile money operators and that of clients. In such cases, the cyber law can prevent the abuse of clients' information by any individuals or organization.

Moreover, individual unsolicited information could be accessed through the mobile money clients' phone. This is because the majority of the passwords used by the mobile-money users are easy to guess. This degree of complexity is closely associated with both illiteracy and negligence levels. The study observed about 90% of respondents to admit the use of passwords with the combination of either numbers or alphabets only. Some of the mobile-money companies limit the password to four digits. This is a very weak protection and could be the contributing factor to the increasing number of cyber crimes in Tanzania. The cyber law could dictate the complexity of the password used.

Another area which shows a potential for attack is the lack of a regular change of the password by users of the mobile money. Above 55.4% of respondents have never changed their password since registration. Further analysis reveals that 54% of clients who never changed their password have the experience of using mobile money for over 18 months. Again, some are not taking precautions out of ignorance while some are doing out of negligence. Regardless of the factor which may have contributed to a failure to take precautions (for self-protection against information abuse), users are vulnerable and must be protected by the law. The cyber law could impose the maximum time for the password to be used.

In an interview with advocates for criminal cases, respondents had a common acknowledgement of changes attained in the court room on cyber crimes. Initially, the court could not execute cases related to cyber crimes because of a number of reasons: One was the absence of the law to guide the prosecution of online crimes, and the other was the fact that online evidence were not accepted by the court. Nevertheless, noticeable changes have taken place to the extent that the Court of

Tanzania allows a court debate to be conducted through video-conferencing. This is a good progress. Regardless of the absence of the cyber law, the court of Tanzania judge cases about cyber crimes based on international laws and experience from international bodies associated with the nation such as the commonwealth. While this approach provides a temporal measure, a comprehensive and permanent approach is needed.

5.2 Does the nature of control of the Tanzanian mobile money platforms adequately address the challenge of cybercrimes?

The question of whether the nature of controls offered by the Tanzanian mobile money platforms adequately address the challenges associated with cyber crimes need urgent attention. This is because crimes associated with mobile money are increasing annually (figure 1). A proper level of security control to mobile money users allows narrowing the focus of scholars and other stakeholders to technical variables influencing cyber crimes. This discussion regards the mobile money platform to consist two sides: System Administrator and Users.

The nation lacks the cyber law to provide guidance to mobile money operators on how, who and when should the system administrator access the account of the client. It is obvious that these operators make such judgements based on personal intuition or internal organization laws. This situation poses a threat because the majority of the mobile money operators (employees) manage to transfer client's money (electronically) with a simple authorization written by a client on a paper. The information proposes that the same transaction could be effected without authorization from the owner. In this case the safety of the account of the client relies much on the integrity of an employee. In an interview with anonymous employees of the mobile money operating companies, they acknowledged that several incidents were reported where employees with low integrity stole the money from clients.

Another factor which poses security threats to the account of the client is the ability of mobile money administrators to change the password of the client without his intervention. It is unfortunate that in most operators, whenever the client forget the password the assigned employee simply creates another password and send it through clients mobile phone. In the case where the mobile money operator is a bank, the same employee is also able to change the mobile phone number where password credentials are directed. This is attested by my own case where I requested a change to my mobile-money login credentials from a bank through the unregistered email while in a foreign country. Isn't this making the mobile money users vulnerable to criminals (hackers)?

On the other hand, the controls administered to users of the mobile money are weak. Unlike where the online banking is used, the mobile money system does only present the user with a single login window. Optionally, the user could use the login credentials provided earlier to access the second login window through the use of temporal credentials sent through other methods such as emails or phone numbers. While the password for the first window is known to the user, the second must be temporal and be sent automatically to the user (through another phone number or user's trusted email). The other number or email should receive such information because it was registered earlier.

The endless duration for password validity is another area that weakens protection in the mobile money system. The study found that all mobile money subscribers were not demanded by the system to change their password periodically. In most cases, the password was valid for the undefined duration of time. There were cases where the mobile money users ignorantly submitted their login credentials to the mobile money Kiosk operator for help. In such cases, the unlimited life span of the password could pose a threat to the user in case the Kiosk operator decided to temper with the account.

Moreover, the study observed that (in most cases) the mobile money users were supposed to use a four digit standard login credentials (password). The password does not necessitate users to mix characters to improve its strength. The survey found several cases where the year of birth of the user was used as a password. The lack of methods to administer the use of strong passwords by the mobile money users create a room for hackers to break through the mobile money accounts, hence increase cyber crime incidents.

6. Cyber Crimes and Mobile Money Officers' Response to Clients' Queries

The study, thought of the possibility that the efficiency of the response of the mobile money staff to queries from clients relates to the rate of cyber crimes in the country. Initially, the survey found that about 33.9% of respondents were confident that they were secure from the unsolicited use of their information submitted for mobile money use. The low percent of respondents who are confident contributed by individual experience in the miss-use of such information or the current trend of online theft (Nyenyelwa, 2013).

It was further observed that about 43% of respondents perceive employees' of the mobile money companies to operate with low efficiency. The reported low efficiency is due to delayed response to requests submitted to the organization for support. With these statistics, many respondents are not comfortable with the efficiency of

employees who attend them. The study by Snow (2011) provides the evidence that low employees' competency in using ICT equipments is among the reasons for low efficiency in attending queries related to cyber crimes in mobile money. To address the issue of knowledge in technical projects, the organization must conduct technical training which is closely monitored to ensure that the acquired knowledge is practiced (Lubua E. , 2014). It is equally important to acknowledge that the unmonitored activities in the organization may result to such delays. Table 1 shows the association between the perceived level of security and the help desk efficiency toward responding to users.

*Table 1: Correlations- Level of Security*Helpdesk Efficiency*

		Level of security from Unsolicited Use of Client's Information	*Help Desk Efficience*
Level of security from Unsolicited Use of Client's Information	*Pearson Correlation*	*1*	*.327***
	Sig. (2-tailed)		*.008*
	N	*65*	*65*
Help Desk Efficience	*Pearson Correlation*	*.327***	*1*
	Sig. (2-tailed)	*.008*	
	N	*65*	*65*

Additional information to the analysis (Table 1) showed a significant correlation between the efficiency by employees in responding to reported queries and the perceived level of security. The r-value is 0.327 and $p < 0.05$. With these results, the increase of efficiency exerts about 33% of influence to the decrease of cyber crime and vice versa. The increase of the efficiency of employees responding to clients' queries is a proper strategy for addressing the challenge of cyber crimes. A quick attendance of queries would prevent crimes which were about to occur. The mobile money companies should assume the role of the natural Police Force, in preventing online crimes to occur while responding to the needs of rescue from users.

Data collected through experimentation showed that the mobile money companies take at least 10 minutes to start responding to a new call from the client. Interviewee complemented these observations by suggesting the presence of some cases where the call made never received a response from the help desk. Some of the mobile money companies have initiated a priority service system, where the client of the mobile money has to pay to receive the priority in services from employees. This is not the right way of doing things, instead clients are to be treated equally and efficiently.

7. Conclusion

The study intended to show how the perceived rate of occurrence of cyber crimes relate to the following factors: the factors are the efficiency of employees in responding to clients' queries, the nature of control by the mobile money platforms and the absence of the cyber law. The study used survey and experimental methods to obtain relevant data. Based on findings presented above, the study concludes that the lack of cyber laws in Tanzania results to the violation of clients' right of confidentiality through allowing employees' and other cyber stakeholders to use clients' information without limit. It increases insecurity to clients because of the lack of protection against online uses of personal information by government entities and business corporations.

Moreover, the study concludes that online platforms of mobile money companies do not address the challenge of cyber crimes adequately because employees are able to interfere with important mobile money information. In online banking, the ability of employees to change the phone number used for online banking by the client, need re-assessment. This is the number where the client receives an authenticating password from the bank. The ability to change such important information must be granted to clients only. Besides, in telecom companies, there must be a separation between the ability to make a new SIM card and mobile money password setting. This will address the challenge of miss-using the information from clients by unfaithful employees. The password complexity must equally be addressed.

It is also necessary for the mobile money employees to increase their efforts in attending queries from clients efficiently. The low rate of response from employees stirs the rate of cybercrimes. Where necessary, employees are to be trained to meet technological needs while ensuring that only competent employees are hired.

References

Aslan, Y. (2006). Global Nature of Computer Crimes and the Convention on Cyber Security. *Ankara Law Review, Vol. 3 No. 2*, 129-142.

Digital Policy Alliance. (2013). *CYBER SECURITY AND E-CRIME WORKING GROUP*. Retrieved May 6, 2014, from http://dpalliance.org.uk/cyber-security-wg/

Genuchten, R. v., Haring, W., Kassel, D. v., & Yakubi, K. (2012). *Mobile phone use in Tanzania.* Amsterdam: vrije universiteit amsterdam.

Intersecurity Magazine. (2013). *Global Cybercrimes Costs.* Retrieved 5 6, 2014, from http://www.infosecurity-magazine.com/view/33569/global-cybercrime-espionage-costs-100500-billion-per-year/

IPP Media. (2014, February 2). *Number of Internet users still low in Tanzania, says global report.* Retrieved June 6, 2014, from http://www.ippmedia.com/frontend/?l=64361

Kumar, N. (2010). *It is estimated that 80 percent of the computers in Africa are already infected with viruses and other malicious* . Retrieved May 6, 2014, from http://www.psfk.com/2010/04/africa-could-become-the-cybercrime-capital-of-the-world.html#!JoaOm

Lubua, E. (2014). *Adoption of E-transparency in the Tanzanian Public Sector.* Durban: University of KwaZulu Natal.

Lubua, E., & Maharaj, M. (2012). ICT Policy and E-transparency in Tanzania. *IST-Africa.* Dar Es Salaam: IIMC International Information Management Corporation.

Mayunga, J. (2013). *Cybercrimes Investigation in Tanzania.* Morogoro: Mzumbe University.

Msuya, N. (2014, June 4). Online Evidence are Accepted by the Tanzanian Court. (E. Lubua, Interviewer)

Ndulu, B. (2012). *Mobile money transactions top TZS1.7tn.* Retrieved May 08, 2014, from http://www.telegeography.com/products/commsupdate/articles/2012/12/13/mobile-money-transactions-top-tzs1-7tn-bank-of-tanzania-reports/

Nyenyelwa, F. (2013, December 15). Security Confidence. (E. Lubua, Interviewer)

Nyerere, J. (1967). *Education for Self-Reliance.* Dar Es Salaam: Government Press.

Pladna, B. (2008). *The Lack of Attention in the Prevention of and How to Improve It.* Greenville: University of East Carolina.

Singer, P., & Friedman, A. (2014). *Cyber Crimes and Cyber War.* New Yorl: Oxford Press.

Snow, G. (2011). *Cyber Security Threats.* Retrieved May 2, 2014, from http://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism

Tanzania National ICT Policy. (2003). *National ICT Policy.* Dar Es Salaam: The Government of Tanzania.

Tanzania Police Force. (2012). *Annual Crime Report.* Dar Es Salaam: Police Force.

Zickuhr, K. (2012). *Digital differences.* Retrieved May 6, 2014, from http://www.pewinternet.org/2012/04/13/digital-differences/

This paper may be cited as:

Lubua, E. W., 2014. Cyber Crimes Incidents in Financial Institutions of Tanzania. *International Journal of Computer Science and Business Informatics, Vol. 14, No. 3, pp. 37-48.*