Tanzania Journal of Engineering and Technology 2022, **41(2)**:189-204
OPEN ACCESS articles distributed under Creative Commons Attribution Licence [CC BY-ND]
Websites: https://www.ajol.info/index.php/tjet, https://tjet.udsm.ac.tz

ISSN 1821-536X (**print**); ISSN 2619-8789 (**electronic**)
DOI: 10.52339/tjet.v41i2.792

Full Length Research Paper

Cyber Security Challenges, its Emerging Trends on Latest Information and Communication Technology and Cyber Crime in Mobile Money Transaction Services

Hakeem J. Pallangyo
St. Joseph University in Tanzania,
Corresponding author: hakeempallangyo3@gmail.com

ABSTRACT

This paper investigates the challenges emerging trends on latest Information and Communication Technology and cybercrime in mobile money transaction services in Tanzania. The objective of this is to evaluate the challenges associated with this rapid growth in ICT and to determine factors influencing Cybersecurity readiness and Cybercrimes in mobile money transaction services. Cyber Security plays a significant role in the field of Information and Communication Technology especially on mobile money transaction services. The study recognizes the provision of mobile money services by both telecommunication companies and local banks, the fact is that whenever we think about the cyber security, the first thing that comes to our mind is "cybercrimes**" which are increasing extremely day to day and become a threat. Cybercrimes are mostly practiced through both internet and mobile money services. Securing the information has become one of the major challenges in the present day. Various Governments and companies are taking measures in order to prevent these cybercrimes. Besides cyber security remains concern to many. This paper mainly focuses on challenges faced by cyber security on the latest information and communication technology and cybercrime especially in mobile money transaction services in Tanzania. Its latest techniques, ethics and trends that change the face of cyber security. Relevant data was collected from the Forensic Section of the Tanzania Police Force, Mobile banking mobile money agents and users of the mobile-money services. This study also used the Pearson correlation and analysis of variance (ANOVA) to establish different facts and determine whether the independent variables had a combined effect on the dependent variable. The findings of the study revealed that there is a positive and significant correlation between users' awareness, mobile money agents training, top management support, technical and logical controls and cybersecurity readiness. The study also concluded that effective training programs aimed to enlighten the users and mobile money agents on cybersecurity issues are an important ingredient for cybersecurity readiness in cybercrime in mobile money transaction services.**

ARTICLE INFO

Submitted: **Dec. 30, 2020**

1st revision: **Dec. 20, 2021**

2nd revision: **June 7, 2022**

Accepted: **June 25, 2022**

Published: **30 June, 2022**

Keywords: *Cyber security readiness, cyber-crime, cyber ethics, mobile money agents, social media, cloud computing, android apps.*

INTRODUCTION

Information and Communication Technology as a modern tool or means of communication, sending and receiving various forms of data with little or no concern on data or information security by the majority of common users. Internet technology is rapidly growing from day to day and many other latest technologies which are altering the face of the people. But due to these emerging technologies we are somehow not that able to protect our private information in a very effective way and hence cybercrimes are increasing every single day.

Today more than 60 percent of total commercial transactions are done online or through mobile money transaction services. Thus, the field of Information and Communication Technology requires an advanced quality of security for real secured transactions since cybercrime has become a big threat. The scope of cyber security is not just limited to secure data or information in ICT industry but also to various fields such as cyber space, data science, database management systems, web and internet technologies, cloud computing, mobile computing, E-commerce and other more needs an advanced level of security.

The enablement impact of mobile money services has seen the percentage of Tanzanian citizens using formal financial services increase from 16% to 65% between 2009 and 2017.4

As of June 2021, Tanzania had 33.2 million mobile money accounts relying on a network of agents managing transactions across rural and urban areas. (TCRA Statistics report 2021)

Cybercrime or computer-oriented crime is a crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Cybercrime may threaten a person, company or a nation's security and financial health (Moore, R. 2005). The U.S. Department of Justice expands the definition of cyber-crime to include any illegal activity that uses a computer for the storage of evidence. The growing list of cyber-crimes includes crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism which have become as major problem to people and nations. (Chris Kim; Barrie Newberger; Brian Shack 2012)

***Cyber Security*:** Cybersecurity is also known as Computer security or information technology security (IT security) is the protection of computer systems and networks from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. (Schatz, Daniel; Bashroush, Rabih; Wall, Julie 2017)

The field is becoming more important due to increased reliance on computer systems, the Internet and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of "smart" devices, including smartphones, televisions, and the various devices that constitute the "Internet of things". Owing to its complexity, both in terms of politics and technology, cybersecurity is also one of the major challenges in the contemporary world.

METHODS AND MATERIALS

Description of the case 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. (Lubua, E. W., 2014)

In the United Kingdom, about 1/3 of internet subscribers are not shopping online due to fear of online security. Cybercrimes reduce the confidence of consumers about the level of online security facilitated by service providers (Digital Policy Alliance, 2013).

A report (sponsored by McAfee), published in 2014, estimated that the annual damage to the global economy was $445 billion. Approximately $1.5 billion was lost in 2012 to online credit and debit card fraud in the US. In 2018, a study by Center for Strategic and International Studies (CSIS), in partnership with McAfee, concludes that close to $600 billion, nearly one percent of global GDP, is lost to cybercrime each year.

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 cybercrimes. However, the impact of cybercrimes 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 cybercrimes 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.

Table 1: USA Jan – June 2012-2013 Crime & Safety Report

Incidents	**Jan-June 2012**	**Jan – June 2013**	**% Increase / (decrease)**
Fraud	2439	2490	2
Intrusion	2203	1726	(22)
Spam	291	614	111
Malicious code	353	442	25
Cyber Harassment	173	233	35
Content related	10	42	320
Intrusion attempts	55	24	(56)
Denial of services	12	10	(17)
Vulnerability reports	45	11	(76)
Total	**5581**	**5592**	

The above report is mentioned as a Comparison of Cyber Security Incidents reported to Cyber in 2013 in USA from January–June 2012 and 2013 in comparison to Tanzania and it clearly exhibits the cyber security threats. As crime is increasing even the security measures are also increasing. According to the survey of U.S. technology and healthcare executives nationwide, Silicon Valley Bank found that companies believe cyber-attacks are a serious threat to both their data and their business continuity.

Companies are maintaining or increasing their cyber security resources and of those, half are increasing resources devoted to online attacks this year. The majority of companies are preparing for when, not if, cyber-attacks occur Only one-third are completely confident in the security of their information and even less confident about the security measures of their business partners.

The number of malware specimens for Macs would continue to grow, though much less than in the case of PCs. Windows 8 will allow users to develop applications for virtually any device (PCs, tablets and smart phones) running Windows 8, so it will be possible to develop malicious applications like those for Android, hence these are some of the predicted trends in cyber security.

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 cybercrime 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 cybercrime 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 cybercrimes. Despite these efforts, incidents of cybercrimes 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 cybercrimes.

Therefore, the aim of the study is to evaluate the challenges associated with this rapid growth in ICT and to determine factors influencing Cybersecurity readiness and Cybercrimes in mobile money transaction services. This paper establishes the following: -

i) It improves the knowledge of stakeholders about the adequacy of methods for addressing the challenge of cybercrime in Tanzania and other developing countries. The more important part is where it identifies employees of the mobile money companies, mobile money agents and their clients i.e., end-users 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.

Description of the case study

The study used the Criminal Investigation Department of the Tanzania Police Force as the key source for secondary data about the trend of cybercrimes in Tanzania. Data were extracted from the cybercrime unit of the Police Force. This is the Police Force section where cybercrimes are reported. Moreover, the study interviewed employees, mobile money agents 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 (cybercrime 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.

Data analysis, the researcher also used SPSS to generate quantitative reports which was presented in the form of a table, pie charts, and bar graphs. The researcher used multiple regression analysis to establish the relationship between the independent and dependent variables. This study also used the Pearson correlation and Analysis of Variance (ANOVA) to determine whether the independent variables had a combined effect on the dependent variable. The study ensured that data were collected from original sources and were clearly audited for reliability reasons. The researcher used the following multiple regression analysis model. The model below was used to determine how cybersecurity readiness in cybercrime in mobile money transaction services is influenced by the identified factors.

$$\mathbf{Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \varepsilon}$$

Where: Y= Cybersecurity readiness; β_0 = Constant; β_1, β_2, β_3, β_4 = Regression coefficients; X_1= Mobile money agents training and end users' awareness; X_2 = Cybersecurity related issues; X_3= mobile money companies' support; X_4= Technical and logical security controls; ε = Error term.

Results and discussions

The general objective of this investigation was to evaluate the challenges associated with this rapid growth in ICT and to determine factors influencing Cybersecurity readiness and Cybercrimes in mobile money transaction services within Dar es Salaam region.

This study sought to examine the factors that influence cybersecurity readiness and Cybercrimes in mobile money transaction services. The four specific objectives for the study were to determine the influence of mobile money agents training and end users' awareness, Cyber Security and Related Issues and technical and logical security controls on cybersecurity readiness and Cybercrimes in mobile money transaction services

Mobile money agents Training and End users Awareness

Human beings are considered to be weakest link in cybersecurity. Mobile money agents training and awareness is key in equipping employees with the knowledge they need to protect themselves from cybercrime elements such as social engineering. The findings of the study revealed that a high proportion of financial institutions dealing with mobile money transactions services do not organize training and awareness sessions in relation to cybersecurity for their mobile money agents and end-users.

However, the study further revealed that most of the financial institutions and mobile companies do not train their mobile money agents on cybersecurity risks and threats as well as how they should handle various risks such phishing attacks. The study also disclosed that some of the financial institutions and mobile companies do not train their employees on cybersecurity policies and bests practices while a few of them do.

The study found that most of the financial institutions and mobile companies offer professional training opportunities mostly to their technical personnel, but quite a number of them do not. However, the majority of the financial institutions and mobile companies indicated that ICT mobile money agents within their mobile money agents have been trained on how to use and manage the security technologies that have been implemented within the organization.

Further, the results of regression and correlation analysis revealed that there is a positive and significant correlation between mobile money agents training on cybersecurity readiness and cybercrime affecting their ender users. This implies that an increase in mobile money agents training leads to a significant increase in cybersecurity readiness and cybercrime. In

fact, mobile money agents training and end users were found to be the most significant variable in the study. For more details on finding see the table 2 below.

Table 2: Summary on findings on agents training and their challenges

Factors	Agree	Strong agree	Neutral	Disagree	Strong disagree
Lack of identification documents	11(12%)	79(88%)			
Low level of mobile money education	9(9%)	82(91%)			
Education on cyber-security awareness	8(9&)	85(94%)			
ICT basic knowledge on security	51(58%)		23(25%)	16(17%)	
Theft from less trusted network operator	12(13%)	71(79%)	7(8%)		
High taxation charges	51(58%)		23(25%)	16(17%)	

Source: field data 2021

From the above table 4; 11, shows that respondents were asked to a Likert scale showing challenges faced mobile money agents especially women who conducting their business at Kariakoo area in Ilala. The liker scale was (agree, strongly agree), Neutral and disagree and strongly disagree where the results indicate that 36% of respondents had disagreed and 64% had strongly disagreed. Therefore, 90 respondents' equivalent to
100% had generally disagreed that lack of easy access to mobile money is not challenge faced by mobile money agents who conducting their business at Kariakoo area in Ilala. This point had also concurred by Tanzi (2016). Said, that currently the mobile money agents are located every Corner of the country and make easy access to mobile money services for those people who excluded from the formal banking system in the country due to the massive revolution of mobile technology in Tanzania but 94% of the respondents strongly agreed that lack of education on cyber-security awareness is their big challenge.

.

Cyber security and related issues

The Government of Tanzania through the Law Reform Commission has circulated a discussion paper on the introduction of legal framework for electronic commerce in Tanzania. The discussion paper came as a result of a study which highlighted lack of relevant legislations for electronic transactions. Two areas have been highlighted in the discussion paper namely contracts and consumer protection. Generally, the legal system in Tanzania is mainly based on Common law. Regulatory steps to secure electronic transactions such as digital signatures, electronic evidence, reforms to contract law, dispute settlement and others have not yet been promulgated. (Tanzania Cybersecurity country report 2005)

The goal of the 2016 Tanzanian report was to explore the evolving threat landscape and the thousands of cyber-attacks that have been forged against individuals, SMEs and large organizations within Tanzania. Cybercriminals continue to take advantage of the vulnerabilities that exist within systems in Tanzania and the low awareness levels. This survey identifies current and future cyber security needs within Tanzanian organizations and the most prominent threats that they face. (Tanzania cybersecurity report 2016)
According to the report of 2016, the respondents who participated in the survey included technical respondents (predominantly chief information officers, chief information security officers, IT managers and IT directors) and non-technical respondents (procurement managers, senior executives, board members, finance professionals, HR professionals and office managers). Thus, the survey measures the challenges facing Tanzanian organizations and the security awareness and expectations of their employees.

Cybersecurity readiness

The study established that the four objectives positively affected cybersecurity readiness. The findings indicated that, by putting into consideration the four factors all indicators associated with cybersecurity readiness that is detection, response and prevention will be boosted and this is a sentiment shared by some of the respondents. Majority of the respondents indicated that their organizations were adequately prepared to detect, respond and mitigate cyberattacks. However, it is important to note that there are other factors (38.9%) not studied in this study that contributes to the cyber-security readiness to end-users. Such factors may include organizational culture among others.

Cybercrime 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 offer 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 cybercrimes.

In 2012, about 627 cybercrime cases were reported. Figure 1 below shows the trend of cybercrimes as reported to the Foreigscic section of the Tanzanian Police Force. There is a steady increase of cybercrimes in Tanzania from 2009 to 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.

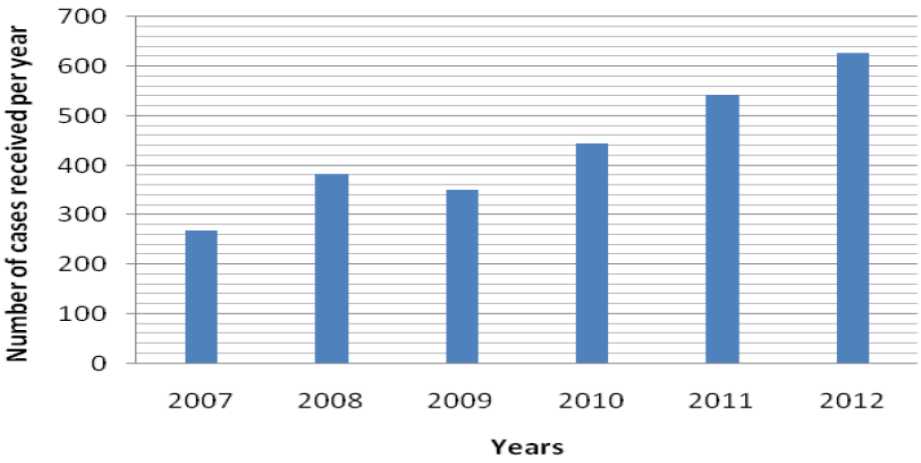

Figure 2: Cybercrimes trends in Tanzania (Tanzania Police Force, 2012)

Cyber Law

Tanzania adopted her first National ICT Policy in 2003. It aimed at increasing the step 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 cybercrimes. 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 an interview with advocates for criminal cases, respondents had a common acknowledgement of changes attained in the court room on cybercrimes. Initially, the court could not execute cases related to cybercrimes 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. (Lubua, E. W., 2014).

Nowadays there is The Tanzania Cybercrimes Act of 2015, was enacted by the National Assembly of Tanzania in April 2015, and signed into law by the fourth president of the United Republic of Tanzania, Jakaya Mrisho Kikwete on 25 April 2015. The law makes provisions for criminalizing offences related to computer systems and Information Communication Technologies; provides for investigation, collection, and use of electronic evidence in Tanzania Mainland and Zanzibar, except to article 50 which do not operate on the Zanzibar. The Law further criminalizes and penalizes a number of cyber activities such

as data espionage, publication of child pornography, publication of pornography, publication of false, deceptive, misleading or inaccurate information, production and dissemination of racist and xenophobic material, initiating transmission of or re-transmission of unsolicited messages and violation of intellectual property rights and other types of cybercrimes. This long-awaited law came after significant impacts such as financial loss, fraud and cyber bullying to the public and other stakeholders.

Tanzanian mobile money transaction service platforms and the challenge of cybercrimes

The nature of control offered by the Tanzanian mobile money platforms its challenge associated with cybercrimes needs urgent attention. This is because crimes associated with mobile money are increasing annually (figure 2). A proper level of security control to mobile money users allows narrowing the focus of scholars and other stakeholders to technical variables influencing cybercrimes. This discussion regards the mobile money platform to consist two sides: System Administrator and Users.

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 clients 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. (Lubua E., 2014).

Moreover, the study observed that the mobile money users were supposed to use a four digits 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 cybercrime incidents.

Cybercrimes and Mobile Money Mobile money agents' Response to Clients' Queries

The study thought of the possibility that the efficiency of the response of the mobile money mobile money agents to queries from clients relates to the rate of cybercrimes 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).

The study by Snow (2011) provides the evidence that low employees' competency in using ICT equipment is among the reasons for low efficiency in attending queries related to cybercrimes 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 3: Correlations- Level of Security *Helpdesk Efficiency

		Level of security from unsolicited client's information	Help desk efficiency
Level of security from Unsolicited Use of Client's Information	Pearson Correlation Sig. (2-tailed) N	1 65	327** 008 65
Help Desk Efficiency	Pearson Correlation Sig. (2-tailed) N	327 008 65	1 65

Additional information to the analysis (Table 2) 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 cybercrime and vice versa. The increase of the efficiency of employees responding to clients' queries is a proper strategy for addressing the challenge of cybercrimes. 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.

Trends Changing Cyber Security

Here mentioned below are some of the trends that are having a huge impact on cyber security. (G.Nikhita Reddy, G.J.Ugander Reddy 2014).

Web servers

The threat of attacks on web applications to extract data or to distribute malicious code persists. Cyber criminals distribute their malicious code via legitimate web servers they've compromised. But data-stealing attacks, many of which get the attention of media, are also a big threat.

Now, we need a greater emphasis on protecting web servers and web applications. Web servers are especially the best platform for these cyber criminals to steal the data. Hence one must always use a safer browser especially during important transactions in order not to fall as a prey for these crimes.

Cloud computing and its services

These days all small, medium and large companies are slowly adopting cloud services. In other words, the world is slowly moving towards the clouds. This latest trend presents a big challenge for cyber security, as traffic can go around traditional points of inspection. Additionally, as the number of applications available in the cloud grows, policy controls for web applications and cloud services will also need to evolve in order to prevent the loss of valuable information. Though cloud services are developing their own models still a lot of issues are being brought up about their security. Cloud may provide immense opportunities but it should always be noted that as the cloud evolves so as its security concerns increase.

APT's and targeted attacks

APT (Advanced Persistent Threat) is a whole new level of cyber-crime ware. For years network security capabilities such as web filtering or IPS have played a key part in identifying such targeted attacks (mostly after the initial compromise). As attackers grow bolder and employ more vague techniques, network security must integrate

with other security services in order to detect attacks. Hence one must improve our security techniques in order to prevent more threats coming in the future.

Mobile Networks

Today we are able to connect to anyone in any part of the world. But for these mobile networks security is a very big concern. These days' firewalls and other security measures are becoming porous as people are using devices such as tablets, phones, PC's etc. all of which again require extra securities apart from those present in the applications used. We must always think about the security issues of these mobile networks. Further mobile networks are highly prone to these cyber-crimes a lot of care must be taken in case of their security issues.

IPv6: New internet protocol

IPv6 is the new Internet protocol which is replacing IPv4 (the older version), which has been a backbone of our networks in general and the Internet at large. Protecting IPv6 is not just a question of porting IPv4 capabilities. While IPv6 is a wholesale replacement in making more IP addresses available, there are some very fundamental changes to the protocol which need to be considered in security policy. Hence it is always better to switch to IPv6 as soon as possible in order to reduce the risks regarding cyber-crime.

Encryption of the code

Encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read them. In an encryption scheme, the message or information is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Encryption at a very beginning level protects data privacy and its integrity. But more use of encryption brings more challenges in cyber security. Encryption is also used to protect data in transit, for example data being transferred via networks (e.g., the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercoms etc. Hence by encrypting the code one can know if there is any leakage of information. Hence the above are some of the trends changing the face of cyber security in the world. The top network threats are mentioned in below.

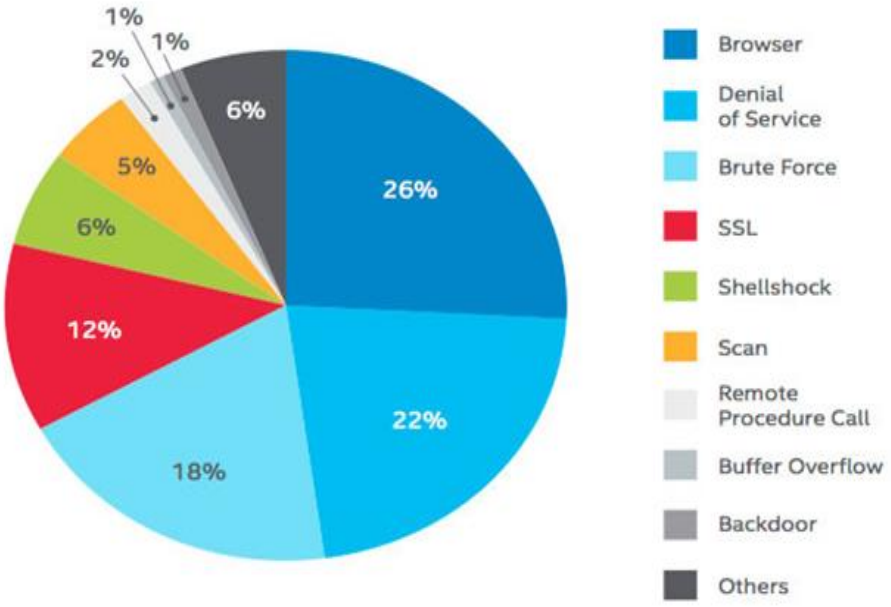

Figure 2: Top network attacks (Source: McAfee Labs 2015)

The above pie chart shows about the major threats for networks and cyber security.

Role of Social Media in Cyber Security

As we become more social in an increasingly connected world, companies must find new ways to protect personal information. Social media plays a huge role in cyber security and sometimes contribute a lot to personal cyber threats. Social media adoption among personnel is skyrocketing and so is the threat of attack. Since social media or social networking sites are almost used by most of them every day it has become a huge platform for the cyber criminals for hacking private information and stealing valuable data. (Lubua, E. W., 2014)

In a situation where we're quick to give our personal information for our benefits, companies have to ensure they're just as quick in identifying threats, responding in real time, and avoiding a breach of any kind. Since people are easily attracted by these social media the hackers use them as a bait to get the information and the data they require. Hence people must take appropriate measures especially in dealing with social media in order to prevent the loss of their information.

The ability of individuals to share information with an audience of millions is at the heart of the particular challenge that social media presents to businesses. In addition to giving anyone the power to disseminate commercially sensitive information, social media also gives the same power to spread false information, which can be just being as damaging. The rapid spread of false information through social media is among the emerging risks identified in Global Risks 2013 report.

Though social media can be used for cybercrimes these companies cannot afford to stop using social media as it plays an important role in publicity of a company. Instead, they must have solutions that will notify them of the threat in order to fix it before any real damage is done. However, companies should understand this and recognize the importance of analyzing the information especially in social conversations and provide appropriate security solutions in order to stay away from risks. One must handle social media by using certain policies and right technologies and the Cybercrimes Act of 2015.

CYBER SECURITY TECHNIQUES

Access control and password security

The concept of user name and password has been fundamental way of protecting our information. This may be one of the first measures regarding cyber security.

Authentication of data

Authentication of date should be checked if it has originated from a trusted and a reliable source and that they are not altered. Authenticating of these documents is usually done by the antivirus software present in the devices. Thus, a good antivirus software is also essential to protect the devices from viruses.

Malware scanners

This is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.

Firewalls

A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. All messages entering or leaving the internet pass through the firewall present, which examines each message and blocks those that do not meet the specified security criteria. Hence firewalls play an important role in detecting the malware.

Anti-virus software

Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. An antivirus software is a must and basic necessity for every system.

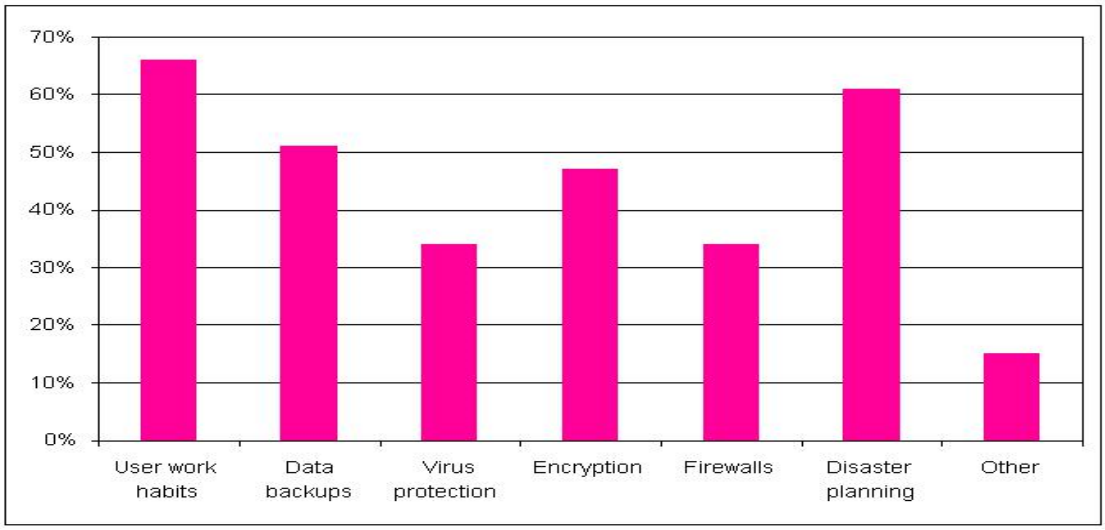

Figure 3: Techniques on cyber security

CYBER ETHICS

Cyber ethics are nothing but the code of the internet. When we practice these cyber ethics there are good chances of us to use the internet in a proper and safer way in respect with The Tanzania Cybercrimes Act of 2015.

The Tanzania Cybercrimes Act of 2015, was enacted by the National Assembly of Tanzania in April 2015, and signed into law by the fourth president of the United Republic of Tanzania, Jakaya Mrisho Kikwete on 25 April 2015. The law makes provisions for criminalizing offences related to computer systems and Information Communication Technologies; provides for investigation, collection, and use of electronic evidence in Tanzania Mainland and Zanzibar, except to article 50 which do not operate on the Zanzibar. The Law further criminalizes and penalizes a number of cyber activities such as data espionage, publication of child pornography, publication of pornography, publication of false, deceptive, misleading or inaccurate information, production and dissemination of racist and xenophobic material, initiating transmission of or re-transmission of unsolicited messages and violation of intellectual property rights and other types of cybercrimes. This long-awaited law came after significant impacts such as financial loss, fraud and cyber bullying to the public and other stakeholders.

Below are a few cyber ethics:

- Do use the internet to communicate and interact with other people in unacceptable manner. Email and instant messaging make it easy to stay in touch with friends and family members, communicate with work colleagues, and share ideas and information with people across town or halfway around the world in a good way.
- Don’t be a bully on the Internet. Do not call people names, lie about them, send embarrassing pictures of them, or do anything else to try to hurt them.

- Internet is considered as world's largest library with information on any topic in any subject area, so using this information in a correct and legal way is always essential.
- Do not operate others accounts using their passwords.
- Never try to send any kind of malware to other's systems and make them corrupt.
- Never share your personal information to anyone as there is a good chance of others misusing it and finally you would end up in a trouble.
- When you're online never pretend to the other person, and never try to create fake accounts on someone else as it would land you as well as the other person into trouble.
- Always adhere to copyrighted information and download games or videos only if they are permissible and.
- Always respect the cyber laws on the country in order to avoid problems.

The above are a few cyber ethics one must follow while using the internet. We are always thought proper rules from out very early stages the same here we apply in cyber space.

CONCLUSION

The study concludes that rate of occurrence of cybercrimes increase due to the following factors: Mobile bank mobile money agents lack enough ICT skills on proactive cybercrime protection measures in responding to clients' queries, the nature of control by the mobile money platforms and lack of enough education on cyber security and cybercrime indications to our people especially end users. People are not aware of the newly Tanzania Cybercrimes Act of 2015, that was enacted by the National Assembly of Tanzania in April 2015 which makes provisions for criminalizing offences related to computer systems and Information Communication Technologies; provides for investigation, collection, and use of electronic evidence in Tanzania Mainland and Zanzibar.

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' awareness results to the violation of clients' right of confidentiality through allowing employees or mobile transaction service mobile money agents and other cyber stakeholders to use clients' information without limit. It increases insecurity to clients because of lack of clients 'protection right awareness 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 cybercrimes adequately because some of employees or mobile transaction service mobile money agents are able to temper with important mobile money information.

Every 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 or mobile money agents. The password complexity must equally be addressed.

REFERENCES

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.

Moore, R. (2005) "Cybercrime: Investigating High-Technology Computer Crime, "Cleveland, Mississippi: Anderson Publishing

Tanzania Communications Regulatory Authority. Quarterly Communications Statistics 2021

Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. 12 (2). ISSN 1558-7215

G. Nikhita Reddy, G.J.Ugander Reddy (2014) a Study of Cyber Security Challenges and Its Emerging Trends On Latest Technologies

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.

Inter-security 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.

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/

"Grand Challenges – Secure Cyberspace", Engineeringchallenges.org, 2017. [Online]. Available: http://www.engineeringchallenges.org/9042.aspx. [Accessed: 09- Mar- 2017]

M. Owens and D. Simpson, Security in Cyberspace, 1st ed. Hauppauge: Nova Science Publishers, Inc., 2013.

Y. Xiang, Cyberspace safety and security, 1st ed. Heidelberg: Springer, 2012.

A Sophos Article 04.12v1.dNA, eight trends changing network security by James Lyne.

Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole

Computer Security Practices in Non-Profit Organizations – A Net Action Report by Audrie Krause.

A Look back on Cyber Security 2012 by Luis corrons – Panda Labs.

International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 Page nos.68 – 71 ISSN 2229-5518, "Study of Cloud

Computing in HealthCare Industry "by G. Nikhita Reddy, G.J. Ugander Reddy

IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013.

CIO Asia, September 3rd, H1 2013: Cyber security in Malasia by Avanthi Kumar.

Tanzania: Cybercrimes Bill Enacted, Global Legal Monitor". www.loc.gov. Goitom, Hanibal. 2015-06-15. Retrieved 2017-09-06.

Cybercrimes Act 2015". Tanzanialaws.com. Archived from the original on 2017-09-12. Retrieved 2017-09-04

American Criminal Law Review Volume: 49 Issue: 2 Dated: Spring 2012 Pages: 443-488

Author(s) Chris Kim; Barrie Newberger; Brian Shack Date Published 2012.