A Rule-based Approach for Resolving Cybercrime in Financial Institutions: The Tanzania case

George S. Oreku
The Open University of Tanzania
george.oreku@gmail.com

ABSTRACT

It is widely accepted that technology is an agent of change in the society. However, the current rate of change in technology, particularly ICT, mobile and ATM machines, leaves room for it to be exploited and be used for things it was not meant for. The paper aims at examining the challenges to electronic banking and initiatives taken to address cyber-crimes among financial institutions in Tanzania. Using the data gathered based on employed comparative analysis methods from our studies and research undertaken by researchers, we examine in detail, technical factors that are continually shaping the landscape of cybercrime and its impact on financial Institutions. Picking a leaf on how to deal with challenges brought by information and communication technology-induced innovations in the banking sector a Platform for Organization Security Threat Analytic and Management (POSTAM) approach to address the cyber security problems in Tanzania was re-introduced. The data model approach was used to analyze collected data stored from the survey to test the security prototype developed.

Key Word: Cybercrime; model; legislation; cyber-attacks; security

INTRODUCTION

The security study literature has shown that system's users are the weak link for security breaches (Anagement, 2010) and therefore hackers use this loop hole to break the system for their personal gain or otherwise. Despite the user being a weak link, the advancement in computer technology also produces a huge amount of data i.e., information overload compared to the organizational ability to manipulate in order to extract potential useful information for informed decision-making (Mbowe et al 2014) and (Mijatov et al, 2013). According to (Mbowe et al 2014) the security awareness and maturity level for selected organizations in Tanzania are not satisfactory in many aspects.

Acknowledgements: The author acknowledges Tanzania Police Defense Force (TPDF), which provided platform for conducting research and archival data sources used by the study.

Electronic banking In Tanzania (or e-banking) has grown largely different from previouslyyears of an overwhelming response in its applicability and reception. Apart from the banks, other financial institutions have also adopted new methods of electronic financial transactions. The adoption of the Automated Teller Machines (ATMs) by various banks and financial institutions and mobile banking by various communication companies such as Tigo, Vodacom and Airtel have encouraged the adoption of habits for deposits and quick transfers of money or payments via electronic payment services (Kato, 2019). The adoption of electronic banking by (CRDB, 2020) (NMB, 2020) (DCB, 2020) Exim Bank and (NBC 2020) for example, confirms the development of electronic banking in the country.

It was noted that, the top management (e.g., directors, managers, supervisors or executive officers exercising the organization's powers) considers information security management as a technical issue rather than a business issue, in which there exists little or no close eye from top management to oversee information security compliance. The poor realization of information security as a corporate governance responsibility has promoted the deadly sins of information security management (Vagias, 2006). As a result, it causes the security management imbalances among internal stakeholders due to inadequate security sense and commitment across the organization structure. In this context, security management imbalance is the phenomenon of uncoordinated efforts among top management and security managers in protecting an organization's infrastructure and data and hence with the new era of computing ubiquitous resulting in lots of cyber-attacks. The definition of "cyber-crime", in the Tanzanian context, varies across the industry as it covers a wide scope of overlapping crime committed with the aid of growing technology. These crimes are classified according to how majority of the people involved make use of the internet and technologies to exchange ideas, keep in touch with family and friends, buying and selling products (including online transactions, M-Pesa) and accessing online services. Cybercrime in Tanzania is mainly committed by two groups of people. Namely, those who perform the act without the knowledge that what they are doing is wrong and those who know what

they are doing but are determined to perform the act in order to distract the country's equilibrium through different angles; from destabilizing peace in a country through misuse of social media and other communication media to stealing money through online transactions.

Tanzania has a high rate of cybercrime and hate speech as highlighted in Mtanzania Newspaper, (Mtanzania, 2013) "There is fear of high rate of individuals who made use of the internet to threaten national security (Tanzania) due to misuse of the blogs and social media along with mobile phones to spread hate speech among communities in Tanzania and the number of cyber criminals worldwide has now increased." In the past, there were a few cases where criminals made use of technology to tamper with ATM machines in Tanzania. Nowadays the act is growing faster and the fear among ATM users has increased due to the fact that each day cyber criminals are coming up with new techniques to steal money from ATMs. People were shocked and surprised when the opposition leader spokesman for the Ministry of Communication, Science and Technology announced that the country has lost 892.18 billion Tanzanian Shillings in Cyber-crimes according to the official reports of the police (http://www.tech360magaz.com). Some sophisticated criminals have been stealing money from the Banks directly; 250 million was reported in Mwananchi Newspaper (Mwananchi, 2012), as being stolen from Uchumi Commercial Bank through the ATM's in Moshi region in Tanzania. Cybercrime has become a global threat which needs an urgent attention at national, regional and international level.

"Cyber criminals are always ahead of us," this fact was backed up by the deputy minister for Home Affair's speech by then on opening conference which took place in Tanzania (http://www.thecitizen.co.tz) "Many people are ignorant of cyber-crimes while our police force has low capacity," he said in Arusha where IT specialists, lawyers, police officers and others from the East African region had a meeting to devise ways to tackle the problem. He added that currently there were more than 300 cybercrime cases which are being investigated by the police in Tanzania but admitted the exercise was slow because the police and other agencies were ill-equipped and not conversant with such crimes. The wave of hacking underscores the financial industry's battle to thwart cybercrime and comes as consumers and banks are reeling from several high-profile data breaches at retailers that have exposed millions of credit cards and debit cards to potential fraud. The statistically presentations from the

research carried out presents the general trend of cyber-attacks within the past six years from different regions in Tanzania (Figure 1).

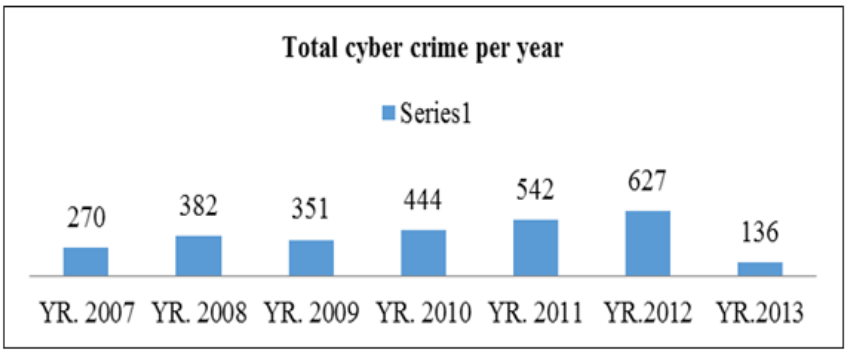


Fig. 1. Cyber crime annual statistics cumulative by 2013. (Source: Tanzanian Cyber Crime Unit 2013)

Criminal Stealing Techniques

From January to April 9, 2015, the number of attacks on debit cards used at ATMs reached the highest level for that period in at least 20 years, according to FICO, a credit-scoring and analytics firm. The company tracks such incidents through its card- monitoring service for financial institutions that represent more than 65% of all U.S. debit cards (Marginally,2015). Debit-card compromises at ATMs located on bank property jumped 174% from January 1 to April 9, compared with the same period last year, while successful attacks at nonbank machines soared by 317%, according to Fair Isaac Corporation FICO (Sidel,2015). The article went further by clarifying that, the incidents come as banks are racing to issue new credit and debit cards with computer chips that make it more difficult for thieves to create counterfeits. However, most ATMs don't yet accept the new technology, though J.P. Morgan Chase & Co. and Bank of America Corp. have recently begun to install the more advanced machines. Criminals send phishing emails or text messages via mobile phones and trick the victims by convincing them to provide their bank details and Automatic Teller Machines (ATM) pins. Using different telephone numbers as request send by the Bank officials requesting some client's details for banks details amendments. Card skimming occurs in the country, whereby cyber criminal's use and record card details by using a device called a "card skimmer" which is placed right over the card slot or over the keypad of the ATM machine and captures card and PIN

information. Web based attacks are becoming more popular in Tanzania which occur when criminals hack websites. Cyber criminals hack the websites to gain unauthorized access to the personal information of clients or web visitors. This in Tanzania imitates how globally the country is positioned in responding to cyber-attacks issues. Hackers are now using the technique to destabilize websites by performing attacks to deny and/or destroy information, steal information, manipulate information, alter the context in which the information is viewed or change the perceptions of people towards the information.

The findings also recognized that there is a case in the Kilimanjaro region in Tanzania concerning theft of money from Mobile Money agents by the same perpetrator (an unidentified female) who is very good at it. She apparently does so by approaching agents pretending to want to draw some money but after a while the agent will find all his money gone after she left the place. It is hard to tell what she does but most of the agents have confirmed that the criminal is the same woman, (Unknown, 2013). Such a report comes after a study that shows that transactions through mobiles are growing rapidly in Tanzania. The use of M-money in Tanzania started in 2005 when Airtel introduced phone-to-phone airtime credit transfer. In 2008 Vodacom launched its M-money service called M-Pesa. Zantel Tanzania also introduced its M-money service in the same year, which was first called Z-Pesa (now called EasyPesa). In 2010, Tigo, the first mobile network operator (MNO) in the country launched its M-money service called TigoPesa. The report by Inter Media in 2013 there are four M-money services brands in Tanzania: M-Pesa, TigoPesa, Airtel Money and EasyPesa. Up to April 2013, the registered customer base of mobile payment services was 28.8 million in Tanzania, 8.5 million being active users Bank of Tanzania (Bank of Tanzania, 2013) Currently, with the new players like Halotel and Tanzania Telecommunications Company Limited (TTCL) Mobile, coming on board by 2016 there were more than 39 million mobile subscribers in the country, of which 16.5 million were mobile money subscribers (Edda et al, 2017)

The weak link that can let a hacker clone the so-called “chip-and-pin” credit and bank cards stems from the fact that use of prepaid debit cards for everything from gift certificates to disaster relief handouts is making it easier for hackers to withdraw large amounts of money before detection (Emily et al, 2018) as the Cambridge researchers showed, the Europay, MasterCard (EMV) scheme has, in too many cases, not been carried out as planned. The authentication process, as originally envisioned, was

supposed to depend on the issuing bank to generate a random number for every unique transaction. In practice, where saving money often trumps security, it was left to point-of-sale terminals or cash machines to generate the number. A large percentage of mobile usage in Tanzania can be attributed to its use as a means of money transfer posing it as a significant threat to become a weak link, as accessibility to mobile money transaction is done through punching in four digits to access the authenticity. This makes it all too easy for a hacker. "If you can predict the number, you can record everything you need from momentary access to a sim card and play it back and impersonate the card at a future date and location (Bond, 2012) The mentioned attacks might seem outdated in developed world but are the most common and fast-growing techniques used by criminals in Tanzania and it is unfortunate that the majority of the population is unaware of this. There have been an increasing number of incidents where victims of credit card fraud had their requests for refunds refused by the issuing banks on the grounds that there is no way to explain the card having been authenticated without the cardholder's involvement. During our research we found that all these are facilitated due to:

The Use of More than One type of Customer ID's

One security weakness of M-Pesa is to allow the use of more than one type of customer ID. For example, a customer who used employer ID to register for M-Pesa account can later withdraw money by using another ID such as driving license, voter's ID or any other ID. This situation makes it possible for an incorrect or forged ID to be used.

Weak Pin

M-pesa PIN is a four-digit number. Moreover, the PIN never expires and is written in plain text during the transaction.

Poor Verification of Customer ID

Another security challenge that M-Pesa agents are facing is on how to authenticate M-pesa customers. The agent usually inspects customer ID physically without having any other mechanism for proving or referencing the validity of that ID from the authorities which issued those IDs. This creates a loophole for a person to register for M-Pesa account with a forged ID.

Poor Transaction Confirmation Procedure

Before a sender completes a transaction, the M-Pesa system requires the sender to confirm each transaction before it is fully executed. For example, when a person withdraws money, the last stage is to confirm the amount of the money to be withdrawn and to whom that money is transferred. Generally, the name of the recipient, amount to be transferred and the account number is displayed for verification. The aim is to avoid wrong or unintended transfer of money. Despite this procedure, several cases of transferring money to unintended recipient have been reported. Inaccurate data entry is the main cause of transferring money to unintended recipient. Some of the reasons that contribute to this problem include poor sender concentration when carrying out the transaction, user illiteracy and unfamiliarity with mobile phones.

Lack of End-to-End Verification

Unlike in banking systems where the bank teller has to verify customer signature and photograph physically and then compare them with electronic copies stored in the system, the agent relies on one side authentication by just examining customer ID. If the customer has forged the ID and places his photo, the agent will not detect it. This loophole allows for a fake customer to use a forged ID to access M-Pesa Services.

Lack of Printed Receipts

Another weakness in M-pesa services is that the agent does not issue a printed receipt to the customer once the money withdrawal or deposit transaction is completed. As already explained, each transaction is issued with a unique receipt number that is included in the confirmation SMS. However, if the SMS is compromised, there will be no evidence to indicate that the transaction was carried out between an M-Pesa agent and a customer. From the analysis above based on our previously findings originated from consolidated research and practical work in the area of cybercrime, emerging perspectives, paradigms and trends which were more based on theoretical aspects mostly (Oreku et al, 2017) deliberate efforts are made in making sure that the role of proposing solutions is undertaken to respond to cyber security problem in Tanzania as additional to what was done previously in research analysis.

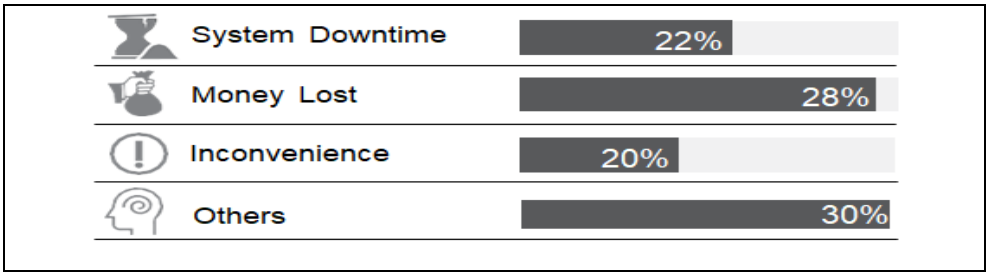
Impact of Cyber Crime

From January to June 2017, 3,340 cases were reported to the police stations. The real impact of the growing interest in fake news however has been the realization that the public might not be well-equipped to separate true information from false information. It is paramount that governments and social media platform owners lay down stringent measures to clamp down on fake news, none the less, we do appreciate that fabricated stories are not likely to go away as they have become a means for some writers to push their narrow agendas, manipulate emotions, make money and potentially influence public opinion. A significant proportion of this cost comes from the insider threat, which we estimate at $30M per annum. In all probability, and in line with our worst-case scenarios, the real impact of Cybercrime is likely to be much greater. As for measuring costs, this report deconstructs the cost based on these four categories:

- ***Costs in anticipation of Cybercrime***, such as antivirus software, insurance and compliance.
- ***Costs as a consequence of Cybercrime***, such as direct losses and indirect costs such as weakened competitiveness as a result of intellectual property compromise.
- ***Costs in response to Cybercrime,*** such as compensation payments to victims and fines paid to regulatory bodies.
- ***Indirect costs*** such as reputational damage to firms, loss of confidence in Cyber transactions by individuals and businesses, reduced public-sector revenues and the growth of the underground economy.

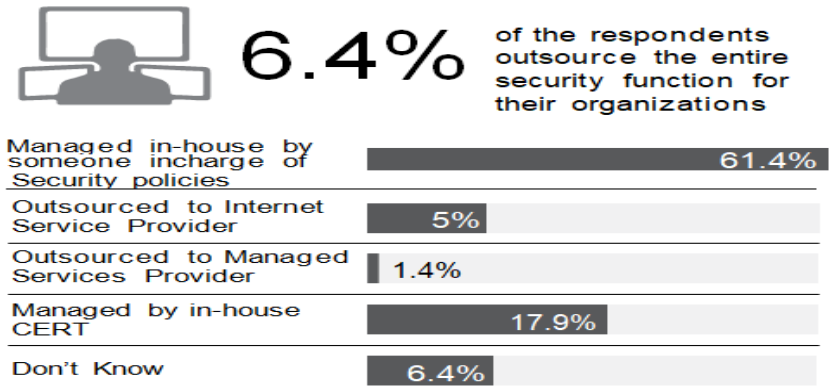
Cybercrime in Financial Institutions

Loss of money, system downtime and inconvenience were identified as the top impacts of cybercrime. This presents one's conclusion that majority of attacks in Tanzania are motivated by financial gain and the reason why Financial Institutions, Savings and Credit Cooperative Societies (SACCOS) and Organization that deal with transaction processing are primary targets for the cyber- attacks. When the study was conducted, particularly with financial institutions, the response to the question, "How has cybercrime impacted you?" majority of respondents indicated an impact of Cybercrime portrayed below.



Managing Cyber Security

79.3% of organizations including Financial Institutions manage their cyber security in-house as follows: - 17.9% being handled by a dedicated in-house Computer Emergency Responses Team (CERT) and 61.4% handled by an individual in charge of security within the organization. This is an increase of 8.3% from the year 2016. Only 6.4% have outsourced these services to an external party managed security service provider and Internet Service Provider (MSSP or ISP). More and more companies are now developing in house capabilities to manage cyber security, this is particularly the case with Banking and financial institutions. Our survey on the question "how is your Organization's cyber-Security being managed" revealed that majority of respondents (55%) who did not know how their cyber security was managed came from the Government sector. This was closely followed by by insurance (11%) then Academia (10%).



Proposed Rule Based Data Mining Model

It is based on the foundation of (Mbowe et al 2016) research work conceptualized in a previously developed prototype which integrated the information security policies to enhance the security strategies for effective protection of critical assets. The generated radar and line graphs for assessing inside threats and security awareness and maturity level in public organization have provided a practical approach for improving the internal security strategies for preserving confidentiality, integrity and availability as core services in security management. After field research and data collections, the study proposed the rule-based data mining approach. Data Mining (DM) has emerged for knowledge discovery especially from big data aimed at predicting the future state of the data for decision making. In so doing, our approach has adopted ruled-based data mining technique for useful information extraction or knowledge discovery (see Figure 2) for visualization of organizational security threats from computer logs, awareness data, security maturity data and other security sources or files.

From traditional DM process model perspective, we have integrated the spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege model (STRIDE) model and organization's security policies into the data mining process model in order to streamline the data mining processes as shown by Figure 7a and 7b contrary to traditional DM approach. By using the classification technique; the security log data, awareness and maturity data were classified at different levels of representation or organizational security threats: spoofing, tempering, repudiation, information disclosure, denial of service and elevated privileges. Five organizations were selected to pilot our approach by testing our model as per table 1 below.

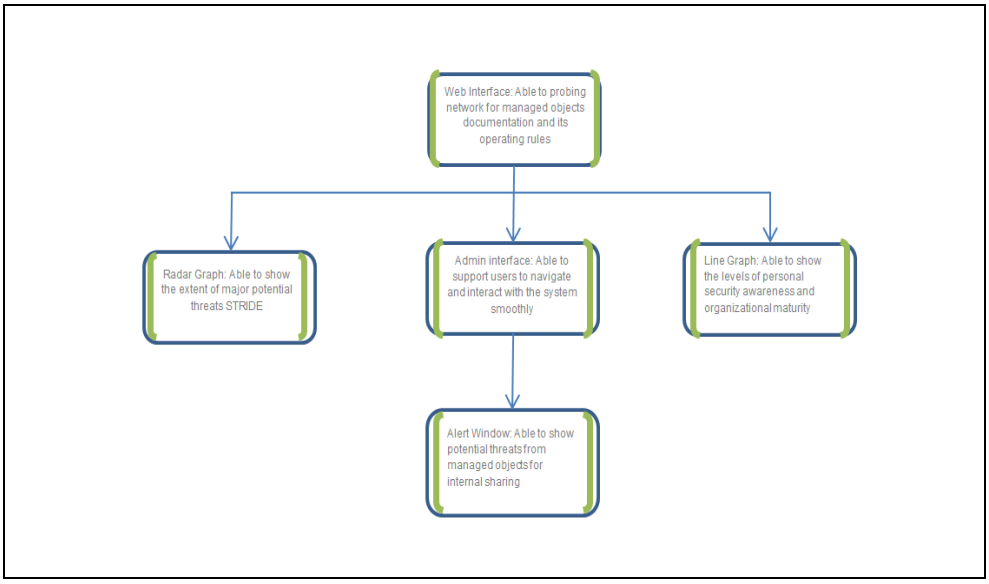


Figure 2. The Conceptual Interface Design Model

Table 1: About 108 participants: 23 IT technical staff and 85 non-IT staff were interviewed using structured questionnaires

Organization	Total Staff	IT staff	Non-IT staff
V	280	14	266
W*	96	3	93
X	236	5**	231
Y	36	4	32
Z	120	4	116
Population	**768**	**30**	**738**
Sample Size(n) C.L=95%, C.I=10		**23**	**85**

**Includes the staff at HQ's only.*
*** Out of 63 IT staff at HQ and up-country, only 5 were drawn from HQ running all critical servers.*

Table 1: About 108 participants: 23 IT technical staff and 85 non-IT staff were interviewed using structured questionnaires.

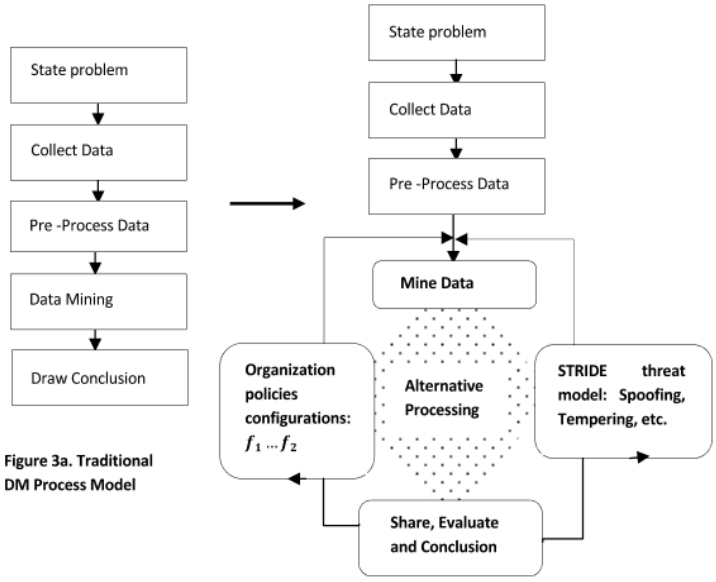


Figure 3a. Traditional DM Process Model

Figure 3b. Processed DM Process Model

To score these organizational security threats, we assessed different levels of the security maturity: non-existence, ad-hoc, repeatable but intuitive, managed and measurable, and finally optimized as indicated by Table 2 and later on the organization's security knowledge and awareness such as non-existence, poor, satisfactory, good, very good and excellent. Furthermore, the Likert-type response anchors (Vagias, 2006) with four possible answers - not at all, a little, quite a lot and completely with compliance numeric value: -0,0.33,0.66 and 1 respectively were used for testing the agreement of compliances of proposed organization's policies for attainment of appropriate security maturity level and security awareness programs. Also, the conversion by (Pederiva, 2003) was used to compute the normalized compliances for the purpose of assessing organization's maturity level and awareness (see Table 2). Thus, predicting the potential organization's threats to be High, Moderate or Low for numeric values 3.33-5.0, 1.67-3.32 and 0.0-1.66 respectively.

Measuring Index	Security Maturity	Security Awareness
0.00 – 0.50	Non-existence	Non-existence
0.51 – 1.50	Ad-hoc	Poor
1.51 - 2.50	Planned	Satisfactory
2.51 – 3.50	Well-defined	Good
3.51 – 4.50	Managed	Very Good
4.51 – 5.00	Optimized	Excellent

2: Security maturity and awareness measuring indicators

Experiment Prototype and Results

After the design phase, the study adopted Web scripting languages and MySQL for web interface and database implementation respectively. The web interface was modeled very simply and intuitively to ensure easy interactivity in security analytic and thus increasing the possibility for wide adaptability across the organization structure. One of the organizations was selected as a case study for experimental prototype implementation. The selected organization has established Information Communication Technology (ICT) policy and its associated ICT information security policy for managing their information assets. However, during data collection we found that its information security policy was based on ISO27001:2005 and thus the controls do not evolve based on organizational risks. Our study adopted ISO27001:2013 information security management framework which rolls based on organizational emerging risks. However, the controls defined by the organization's information security policy were used in order to maintain their existing policy structure. After this technical alignment, the data collected in (Mbowe, 2013) during assessment of security awareness and maturity levels were used as pilot data for testing the experimental prototype while on development stage. The statics of the survey from five companies are presented in the table 1 above.

Prototype Experimentation

The functions provided by the prototype were developed using PHP and R scripting languages. The back-end operations (e.g., analytic engine) was implemented by R scripting language R Core Team (2015) and MySQL database engines. On the other hand, the front-end operations (e.g., web interface for user interactions and data presentation) PHP scripting language was used. The web interface was modeled to be very simple and intuitive to ensure easy interactivity and thus increasing the possibility for wide adaptability across the organization structure.

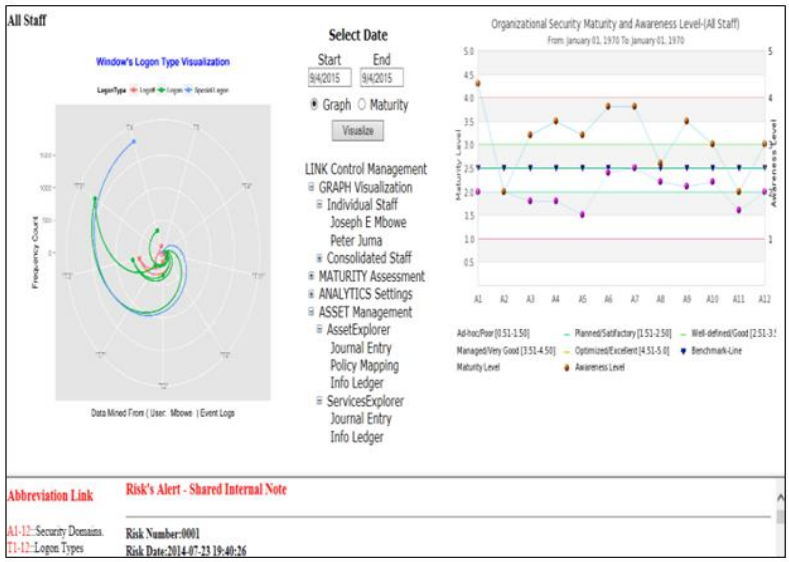


Fig. 4. The panel for visual data representation of experimental results

For experimentation purposes, the organization which was selected as a case study had computer logs collected for analytics and visualization. The output of the prototype is presented by the screen snapshots shown by Figure 4. Our experiment was focused on Windows Logon by analyzing different types of logon or logoff activities prompted by a particular event and thus monitoring unusual logon/logoff for type 2, 3, 8 and 10. The study found that, selected logon types may have high impact on security when window policy configurations are inadequately configured. For example, the check-indicator of each type is described in Table 3.

Table 3: Security maturity and awareness measuring indicators

Logon Type	Description	Check-Indicators
Logon Type 2 - (T2) **Interactive**	A user logged on from console to this computer	Suspicious Type 2 multiple *audit failure* may indicatepassword guess or elevation using console or keyboard.
Logon Type 3 - (T3) **Network**	A user or computer logged on to this computer from the network.	Suspicious Type 3 multiple *audit failure* and later *audit success* may indicate anonymous logon by malware or attacker through a network.
Logon Type 8 - (T8) **NetworkClearText**	The user's password was passed to the authentication package in its un-hashed form with audit success	Type 8 audit success indicate inadequately policy configuration which allows plaintext or clear text as login credentials thus easily to be sniffed.
Logon Type 10 - (T10) **Remote Interactive**	A user logged on to this computer remotely using Terminal Services or Remote Desktop.	As type 3, but user tried to login from remote computer

As shown on Figure 4, the extracted information from window's security logs representing logon/logoff for type 2, 3, 8 and 10 is presented by Figure 5.

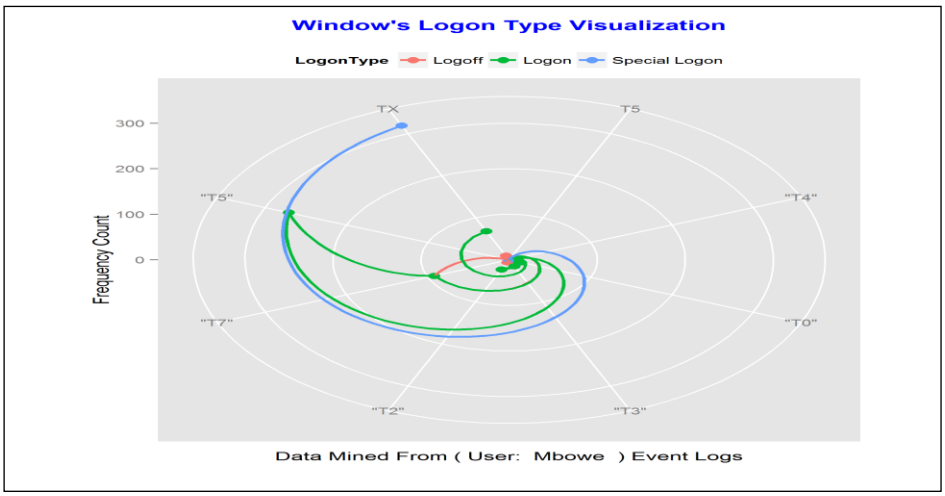


Figure 5. The Security Logs Data Visualization

Prototype Overview

The data visualization using the proposed prototype has shown that it can be useful for leaders, systems administrators and security officers to keep an "eye" on critical systems or computer attached to their cyberspace. Also, the use of pictorial presentation of security logs based on logon types have simplified the visualization of big data such as security logs generated by Windows security logs. For example, the quick-scan of the summary data showed that about 3% (238) of audit failure occurred compared to 97% (7,920) of audit success for a given time interval. Actually, if more Audit failure occurs, it gives an insight for further follow-up to see what is happening in the background to ensure the success or failure is not occurring due to attack through various security loopholes. Also, the processed information presented by the radar graph (see Figure 5) can be used for decision-making in regard to information security management.

The platform also has demonstrated the practical ways for automation of an organization's information security policy for provision of effective strategies for security management. It illustrates the extent of potential inside threats and the user-compliance for a particular organizational environment and culture. Furthermore, it's of our opinion that, the greater understanding of the security awareness across the organization structure will be a catalyst for management accountability to enhance security management. This proposed platform generates graphs and internal risks notifications which can be the source of information for preparing the effective security strategies including security seminars, workshops and training so as to ensure all security domains are well covered to preserve security confidentiality, integrity, accountability and availability.

The Key Findings of the Research

Whilst there was no clear consensus on the trends of cyber security in Tanzania, there was a definite agreement that the top cyber security breaches in Tanzania result from social engineering attacks such as phishing, 419 scams, identity theft and unauthorized access. Breaches resulting in financial fraud and embezzlement through internal collusion and involving e-delivery channels such as ATMs, mobile channels and the web were also rated high, particularly for the financial sector. The third highest category of cyber security breaches is information asset Research by Wolf Park, (2014). Perfecting the findings done previously

in (Oreku et al 2017, & Mbowe et al, 2016) to supplement the foundation put forward. This paper has expanded to reflect the changing emphasis on cyber security extent. Similarly, the small changes and improvements on Theft through session hijacking, email hijacking and website hijacking was also noted throughout. Moreover, respondents rated the internet as the leading source of cyber security breaches in Tanzania, followed by insider collusion, pharming and phishing. Furthermore, the research identified the following results:

- An overwhelming majority of respondents selected social engineering as the key cyber-attack method in Tanzania and also identified malware and key loggers as other frequently used methods.
- For example, from the research conducted, about 92.1% respondents indicated that their organizations had no effective strategies for managing their ICT assets with regard to security breaches and only 41.2% respondents were aware of the existing security awareness programs.
- According to other respondents, they were of the observation that leading cyber vulnerability in Tanzania is the lack of user awareness for both employees and customers. The vulnerabilities arising from weak technical security practices such as poor patch management, outdated anti-virus software and unsecured or misconfigured networks were also highly rated as per our findings.
- According to the survey, the use of monitoring tools and other detection mechanisms could be the principal way of detecting cybercrime threats in Tanzania today. Customer reports also could be the next most prevalent detection method. The use of internal audits and routine staff checks are also key detection methods.
- As currently there is no accurate data addressing the cost of cybercrime cost in Tanzania and most of the loss still goes unreported, the respondents were only able to estimate a conservative loss in excess of 892.18 billion Tanzanian Shillings on Cyber-crimes by the year 2012 annually whilst noting that the key emerging threat to cyber security in Tanzania today is related to e-delivery channels (ATM fraud, mobile fraud & card holder data theft), followed by social engineering attacks.
- However, it is estimated that governments could lose more than USD 50 billion to deal with the costs associated with malware on pirated software by article "'Microsoft Reminds Consumers to be Vigilant to avoid Unintentional Purchase of Counterfeit Software," (2016)
- Respondents from financial institutions and telecoms sectors reported

having in-house staff with requisite Information Security training and certifications. The in-house staff and external service providers used to detect incidents and conduct investigations as experts; though the number of these people was low and hence the need for more experts was paramount.

- Our research also found that many Tanzanian organizations, especially financial institutions, do not report many cybercrime incidents, out of fear of reputation damage. Other reasons include a lack of confidence in the ability of law enforcement agencies to handle cybercrime incidents and the absence of consequences for not reporting cybercrime.
- Many respondents noted the absence of a legal and regulatory framework being in place as a glaring impediment to cyber security in Tanzania. It was, however, noted that the Cybercrime Bill 2013 is awaiting passage by the National Assembly. This bill, together with the existing Task Force (comprising of members from Bank of Tanzania (BoT), Tanzania Communication Regulatory Authority (TCRA), Financial Intelligence Unit (FIU), Tanzania Bankers Association (TBA) and the Police Force Cyber Crime Unit) will have mandate to attain compliance to the ISO27001 and ISO27002 international standards and are regarded as the top initiatives to develop and strengthen Tanzania's legal and regulatory framework.
- Respondents also noted a number of key collaborative initiatives aimed at addressing the cyber threat quandary include the Tanzania Communication Regulatory Authority (TCRA), Police Force Cyber Crime Unit, the UDOM Cyber project, and Professional Association led initiatives. Most respondent organizations participate in various public-private partnerships for the purpose of preventing and detecting cybercrime. However, suggestions were made towards collaborating on a National, Pan- African and International scale. Moreover, respondents felt the need for research to drive these initiatives and combat cybercrime as a whole and this should be driven by public-private partnerships.
- According to the survey, the top skill sets needed in Tanzania are computer and digital forensics, forensics investigation, cybercrime prevention, detection and incident handling and technical ethical hacking skills. Respondents felt that the training needs could best be addressed by a National Cyber Security Training Task Force, in conjunction with private training institutions, which should be properly regulated and accredited.

- The study revealed cyber security related training received by government and regulatory authorities is particularly deficient, whereas, e-payment companies appear to receive adequate training in this regard. Respondents identified various training interventions ranging from general awareness to highly skilled information security courses addressing incident response, attack and defense, secure coding, ethical hacking and forensic investigation.
- An overwhelming majority of respondents do not believe Tanzania is investing enough resources in mitigating cybercrime, although it was noted that considerable investment had been made by Tanzania Communication Regulatory Authority (TCRA), mainly in response to its mandate.
- Most respondents agreed that there should be an inclusive large scale and sustained national awareness campaign on cyber security across the country addressing all stakeholder groups with an emphasis on the key sectors of the economy and targeted at the top tier of organizations.

Further Enhancements of the Prototype

Currently, the prototype includes threats associated with violation of organization information security policy which used for experiment based on ISO 27001:2005 security domains and sample data loaded for STRIDE threats evaluation. However, further work is required to review the existing policy to comply with ISO27001:2013 and also to integrate the automatic assessment of vulnerabilities from security logs and known loop holes associated with malware activities, unmanaged configurations, active Trojan ports and security logs from big data (e.g., security warning and error logs). As part of the future enhancements, the prototype could be developed to be used in other types of threats as well as different operating system apart from Windows only.

CONCLUSION

Cyber security is today without doubt, an issue of national concern demanding urgent, focused and far-reaching measures to address it. Given the results of this paper and lessons learnt on a global, regional and national level we have identified one of the challenges in Tanzania is to build a nation that is aware of the importance of information security. We urge the passing and enforcement of the Cybercrime Bill 2013 to provide a basis for securing the nation's cyber space. Also, we recommend a

national CERT to be an initiative with private sector input. During prototype testing; we selected one organization from five different organizations which participated in the previous study to run the prototype developed. The graphs generated for visual demonstration have provide evidence that, the policies can be automated to support security management based on pre-defined set of rules. The paper encourages the adoption of global best practice standards, with a bias for information security, on a national level to strengthen institutional controls, processes, systems and skills. Taking the lead from the banking regulator, other regulators should follow suit to adopt these standards within their sectors. Taking the lead from the banking regulator, other regulators should follow suit to adopt these standards within their sectors. Key sectors of the economy such as telecoms, public sector, non-bank financial institutions, oil and gas would be a priority as would-be emerging sectors such as mobile and e-payment providers and large retailers.

REFERENCES

Anagement M, et al, (2010) "User Participation in Information Systems," vol. 34, no. 3, pp. 503–522

Bond M, Omar Choudary O, Murdoch S.J, Skorobogatov S., and Anderso R., (2012) "Chip and Skim: cloning EMV cards with the pre-play attack", Computer Laboratory, University of Cambridge, UK

Bank of Tanzania (2013), Monetary Policy Statement 2013/2014, ISSN 08556-6976.

Kato C.I, (2019) "Legal framework challenges to e-banking in Tanzania", Legal Department, Tanzanian President's Office: Public Service Remuneration Board, Dar es Salaam, United Republic of Tanzania, PSU Research Review, ISSN: 2399-1747 Publication date: 29 August 2019

Co-operative Rural Development Bank (CRDB).

Dar es Salaam Commercial Bank (DCB).

Emily F. &, Tanya A., (2013) "Prepaid debit cards: a weak link in bank security" May 11, 2013/8:37am, Accessed on 26 March, 2018

Feschetti M. and Lodi A, (2003) "Mathematical Programming" local Branching, vol.98.

http://www.tech360magaz.com/2012/07/tanzania-lost-89218-billions-on.html line, cited on July 2012.

Krisanthi G. A., Sukarsa I. M.,and Bayupati P. A.,(2014) "Governance Audit of Application Procurement Using COBIT Framework," J. Theor. Appl. Inf. Technol., vol. 59, no. 2, pp. 342–351.

Lwoga T.E., & Lwoga N. B., (2017) "User Acceptance of Mobile Payment: The Effects of User-Centric Security, System Characteristics and Gender", The Electronic Journal of Information Systems in Developing Countries EJISDC, pgs 81, 3, 1-24

Mbowe J.E., Msanjila S.S., Oreku G.S, & Khamisi K. (2016) "On Development of Platform for Organization Security Threat Analytics and Management (POSTAM) Using Rule-Based Approach", Journal of Software Engineering and Applications.

Mbowe J. E., I. Zlotnikova, S. S. Msanjila, and G. S. Oreku, (2014) "A Conceptual Framework for Threat Assessment Based on Organization's Information Security Policy," J. Inf. Secur., vol. 5, no. October, pp. 166–177.

Mijatov S., Langer P., Mayerhofer T., and Kappel G, (2013) "A Framework for Testing UML Activities Based on fUML." in MoDeVVa@ MoDELS, pp. 1–10.

Marginally N, (2015) "Think FICO is a credit scoring company?" Nope: it's about large-scale analytics".

Mtanzania, a local newspaper, cited on July 26, 2013, page 6.

Microsoft Reminds Consumers to be Vigilant to Avoid Unintentional Purchase of Counterfeit Software., (2015) Accessed on 28 may 2016.

Mwananchi Local Newspaper on Monday, cited on 16 July 2012.

National Microfinance Bank (NMB).

National Development Bank.

Oreku G.S, Mtenzi. F.J., (2017), "Chapter 6, Cybercrime: Concerns, Challenges and Opportunities", Springer Nature, 2017.

Pederiva A., (2003) "The COBIT maturity model in a vendor evaluation case," Inf. Syst. Control J., vol. 3, pp. 26–29,

R Core Team (2015). R: "A language and environment for statistical computing", R Foundation for Statistical Computing, Vienna, Austria, URL http://www.R-project.org/.

Researched by Wolf Park, (2014) "The Nigeria Cyber Threat Barometer, report, https://www.wolfpackrisk.com/assets/docs/the-2014-barometer-report.pdf, Accessed on 28 March 2018.

Sidel. R (2015) "Theft of debit-card data from ATMs soars, Thieves are stealing information to make counterfeit plastic" *The Wall Street Journal,* May 19, 2015 7:41 PM

Von Solms B. and. Von Solms R, (2004) "The 10 deadly sins of information security management," Comput. Secur. 23(5), 371–376.

Vagias W. M., "Likert,. (2006) "Type Scale Response Anchors"