International Journal of Scientific Engineering and Science
Volume 2, Issue 4, pp. 40-49, 2018. ISSN (Online): 2456-7361

An Investigation on Issues and Challenges of Information System Security and Its Cryptographic Techniques: A Case Study of Tanzania Revenue Authority Dar Es Salaam

Edward Onyango Orinda[1], Alex Zakaria Ndaba[2]
[1]ICT Consultant and Software Developer & Researcher, Lecturer, School of Applied Science and Technology, Kampala International University in Tanzania
[2]Head of Department and Lecturer School of Applied Science and Technology, Kampala International University in Tanzania

***Abstract* —** *The purpose of the study was to examine the challenges of the information system security and its cryptographic techniques at Tanzania revenue authority. Objectives of the study were; to identify techniques that can be used to secure information systems in organizations, to examine the challenges faced by Tanzania revenue authority in ensuring the security of their information systems and to determine the level of information system security of TRA based on the CIA triangle. The research design used was descriptive cross sectional survey. The study covered the total population of 36 staffs which was purposively sampled from Tanzania revenue Authority employees. Research instrument used was Questionnaire which made it easy to gather data from the field and collect information from the field of study.*

Data analysis was done with help of (SPSS) Statistical Package for Social Science which was used during data manipulation. Findings showed that TRA is using most of the important cryptographic techniques to secure information systems but still are faced by information system security challenges like most system users misuse the system and some users share their usernames and passwords which seems to be serious challenges that may cause occurrence on the system security. It was recommended that the TRA IT administration is required to increase effort in the process of identifying new challenge so as to employ new techniques in the process of securing information systems. Also the IT administration should regulate the system users as they are the main sources of the challenges faced within the organization.

***Keywords* —** *Challenges, Confidentiality, Cryptographic, Information, information System, Integrity, Intrusion Detection System (IDS), Issues , Privacy,Protocals, investigation, Security*.

I. INTRODUCTION

Background of the Study

All over the world information has become a critical asset of all organizations owing to their rapid adoption of IT (Information Technologies) in the entirety of their business activities, which has arisen from the need for the careful management of the organizations information. Information Systems therefore undoubtedly play an important role in today's society and are ever-increasingly at the heart of critical infrastructures, and this is widely accepted in security research literature (Mellado, Blanco et al., 2010). However, information technology is a fruitless effort if there is no security. Information gathered over a period of time can be accessed, stolen or modified in just one second, which renders all efforts invested useless.

According to Pfleeger (1989), Information security refers to the protection of information and communication technologies against attacks. An attack is an intentional threat and is an action performed by an entity with the intention to violate security policies. These attacks could come in form of destruction, modification, fabrication, interruption or interception of data (ISO/IEC 2005).

The current tendency towards using information systems which are increasingly bigger and are distributed throughout the entire Internet has led to the emergence of many new threats to security (Opdahl and Sindre, 2008). This signifies that present-day information systems are vulnerable to a host of threats and cyber-attacks by cyber-terrorists, hackers, etc., such as virus which are propagated through the Internet, social engineering attacks or the inappropriate use of the Net's assets by companies' employees (Choo, Smith et al., 2007). Due to this fact the process of managing secure information is one of the most difficult tasks and challenge to implement and maintain effectively in organization.

Research has shown that the more sophisticated hackers can attack routers and firewalls and change the security controls that an organization has established to keep intruders out. Many astute organizations have risen to this challenge by fighting fire with fire that is, they have established a team of technical specialists that attempt to hack their own systems to discover security holes and to ensure that established controls remain as they were intended (Micki Krause, Harold F. Tipton). Research has also shown that many a times internal employees subvert existing controls to gain undue advantage essentially because either an opportunity exist to do or they are disgruntled (Backhouse and Dhillon, 1995)

Information system security threats are more pronounced in Countries where the computerization level is high, (Carrier, 1994).

Information security damage in the USA as a result of compromised information security systems and damage from computer crimes is five billion dollars yearly, the offenders steal nearly 4 billion euro a year. These crimes are increasingly becoming rampant at an increasing rate of 30-

40% every year (Isaca, 2006). Furthermore, According to the 2007 Computer Crime and Security Survey, conducted jointly by the Computer Security Institute and the San Francisco Office of the Federal Bureau of Investigation, 46 percent of respondents reported some form of security incident during the year 2006 (Richardson 2007). Moreover, security incidents, such as viruses, system penetrations, insider abuse, or other forms of unauthorized access continue to increase in sophistication and impact, with the average annual loss reported by U.S. companies doubling from $168,000 in 2006 to $350,424 in 2007 (Richardson 2007).

In Germany the offenders steal nearly 4 billion euro a year. And the quantity of such crimes is increasing on 30-40% every year. Isaca (2006). Research has also shown that many a times internal employees subvert existing controls to gain undue advantage essentially because either an opportunity exist to do or they are disgruntled(Backhouse and Dhillon, 1995)

In South Africa, the convergence of technologies together with advances in wireless communications, has meant new security challenges for the information security fraternity. As hotspots become more available, and more organizations attempt to rid their offices of "spaghetti" so the protection of data in these environments becomes a more important consideration. It is this fraternity that organizations, governments and communities in general look to for guidance on best practice in this converging world.

Gambia is one African country that has had a fair share of illegal bypasses. People compromised the international gateway of the Gambia Telecommunications Company (Gamcel) thereby defrauding it of huge amounts of money (Africa telecom and IT, 2013).

In east Africa such as in Kenya Cyber threats have been identified as the most pressing challenges to the security of organization whether private or public. Enhancing the security, resiliency, and reliability of the nation's cyber and communications infrastructure is a challenge that must be met. The banking sector is the main target. Cyber Security Africa says security systems risks have been identified as the biggest challenge for many organisations in the region (Kioko, 2013).

In Tanzania the information system and computer technology is still a newer technology, it is becoming increasingly difficult to control access, and maintain integrity and privacy of data. In addition, the increasingly rapid evolution and growth in the complexity of new systems and networks, coupled with the sophistication of changing threats and the presence of intrinsic vulnerabilities, present demanding challenges for maintaining the security of information systems (ICT security guidelines, 2012).

In TRA one of the challenges that facing the organization's system is the viruses due to the lack well management process of mobile electronic devices when connecting to the corporate network to access e-mails. The TRA blocked access to all mobile due to emergence of viruses and other malicious impact. The high cost of downtime due to security concerns had a significant impact on productivity which resulted in a loss of revenue for the agency. The TRA also tried to encrypt company documents to ensure that those would not be accessed by unauthorized users. It is clear that the issues raised by the lack of an effective security solution needed to be addressed in order to comply with regulatory policies (Technical Analyst at the TRA, 2012).

Statement of the Problem

The process of ensuring information system security for one hundred percent seems to be a difficult task for many organizations due to the fact that the development of information technology which continue to grow day by day. This contribute to the growth and increasing of threats which faces information systems that may lead to the stealing, deletion, alteration, destruction or loss of information. Intruders such as hackers and crackers, malicious software such as virus, Trojans, horse and natural hazards such as fire brought a big challenge to secure systems in one hundred percent within the organization. The researcher intends to examine the techniques used by information system intruders to break into and challenges to ensuring information systems security.

Purpose of the study

The purpose of this study is to examine the challenges of the information system security at Tanzania revenue authority.

Research objectives

1) To identify techniques that can be used to secure information systems in organizations.
2) To examine the challenges faced by Tanzania revenue authority in ensuring the security of their information systems.
3) To determine the level of information system security of TRA based on the CIA triangle

Research questions

1) What techniques can be used to ensure security of information systems in organizations?
2) What are challenges faced by TRA in ensuring the security of its information system?
3) What is the level of information system security at TRA?

Scope of the study

Content scope

The study limit its self to determine various challenges that facing information system security at TRA and discussing on solutions that can be applied to overcome information system security challenges.

Geographical scope

The study carried out at Tanzania revenue authority in dar es salaam, Tanzania.

Theoretical scope

The CIA model used to guide the study. CIA triad is an international standard for evaluating information systems security in organizations.

II. Review of Related Literature

Techniques for Securing Information Systems in Organizations

According to Mellado, Blanco and et al.(2010), Information has become a critical asset of all organizations owing to their rapid adoption of IT (Information Technologies) in the entirety of their business activities, which

has arisen from the need for the careful management of the company's information. Information is an asset which is currently as important as capital or work. This reality is even more pressing in new generation companies in which information is part of their core business. In fact, in the last few years we have observed more and more organizations becoming heavily dependent on Information Systems (IS) (Mellado, Fernández-Medina et al., 2007). Information Systems therefore undoubtedly play an important role in today's society and are ever-increasingly at the heart of critical infrastructures, and this is widely accepted in security research literature

Choo, and Smith, (2007) explain that, the current tendency towards using information systems which are increasingly bigger and are distributed throughout the entire Internet has led to the emergence of many new threats to security .This signifies that present-day information systems are vulnerable to a host of threats and cyber-attacks by cyber-terrorists, hackers, etc., such as virus which are propagated through the Internet, social engineering attacks or the inappropriate use of the information system assets by company's employees

According to Opdahl and Sindre, (2008). There are many ways to prevent access to an information system. From physical security involving locks and guards to measures embedded in the system itself. The user is a source of vulnerability and every user represents a way to access the system. Therefore, security measures should begin with users. Information systems security measures can be further categorized into four Preventive measures, this refers to what can be done to prevent security accidents, errors and breaches. Most physical security controls are a key part of prevention techniques, as are controls designing to ensure the integrity of data.

According to Opdahl and Sindre, (2008), detection measures are those measures used for spotting when things have gone wrong. Detection needs to be done as soon as possible particularly if the information is commercially sensitive. Detection controls are often combined with prevention controls for example, a log of all attempts to achieve unauthorised access to a network. Deterrence measures refers to controls used to discourage potential security breaches while Data recovery measures this refers to measures that ensure continuity of the organization even after things have gone wrong. For example, if data is corrupted or hardware breaks down it is important to be able to recover lost data and information.

According to Tony (2006), a Passwords is a secret word or string of characters that is used for user authentication to prove identity, or for access approval to gain access to a resource (example: an access code is a type of password). The password should be kept secret from those not allowed access. The use of passwords is known to be ancient. Sentries would challenge those wishing to enter an area or approaching it to supply a password or watchword, and would only allow a person or group to pass if they knew the password. In modern times, user names and passwords are commonly used by people during a log in process that controls access to protected computer operating systems, mobile phones, cable TV decoders, automated teller machines (ATMs), etc. A typical computer user has passwords for many purposes: logging into accounts, retrieving e-mail, accessing applications, databases, networks, web sites, and even reading the morning newspaper online

According to Tipton (2004), encryption is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can. 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. Any adversary that can see the cipher text should not be able to determine anything about the original message. An authorized party, however, is able to decode the cipher text using a decryption algorithm. There are two basic types of encryption schemes: Symmetric-key and public-key encryption.

According to Berinato (2005), contingency planning is the technique that is crucial to a successful information systems security. This backup plan is based on contingent event. An event that may or may not occur. In the event that it does occur, a plan to get the system up and running as soon as possible will be put into action.

According to Baguméés and Zeidler (2010), off-site Data backup is the technique critical to the ongoing operation of the computer facility. Backups help prepare for uncertainties like fires that might consumes everything, floods, theft and alterations and deletions of data.

According to Allen and Julia (2001), use of annunciation panels. These are used to signal abnormal conditions, including fluctuations in electrical power, low fuel levels in power generators, status of coolant pumps, and unauthorized entry and intrusion. Dial-back devices are used to verify that users at remote terminals are indeed authorised users

According to Dhillon (2000) mantraps are usually sequential-entry double doors or turnstiles at computer room entrances activated by security guards inside the guard station or by key card. Frequently they include key card door locks, audible alarms, closed circuit TV surveillance, and metal detectors. A mantrap generally assists the security guards in detaining a person attempting to enter or leave the computer room until the guards are satisfied that the person is authorized. A guard station is a specifically constructed and designed enclosure that is usually connected to or part of the mantrap. They are equipped to monitor security of the data centre.

According to Karen and Forcht (1994), internal communications include intercom systems linking guard stations and all areas concerned with the daily operation of the data centre. Generally, the system provides guards with override capability of all station, conference calling and busy line indicators. Direct communication with the police is often also provided.

According to Baguméés and Zeidler (2010) smart cards and Biometric devices can also be installed at entries of different computer centres so as to further limit access to computers and data.

Information Systems Security Challenges

The permanent and global nature of security threats and the increasing complexity of IT infrastructures are currently leading organizations throughout the world to revise their approaches towards information security. Hiring Information and Communication Technologies equivalent of military men, i.e. security technologists and white-hat hackers, and entrusting security to them is no longer sufficient. Most organizations fully recognize the need to continuously improve their internal security culture by establishing and maintaining proper security governance processes. However, this is easier said than done. Some international companies still rely on obsolete security standards, such as the ISO/IEC 17799, which were developed when current ICT threats and complexities were still unheard of. The more recent ISO/IEC 27001 standard has finally introduced the notion of a security policy life-cycle; but in today's dynamic ICT environments, emerging threats and sudden changes in technology may require much more agile decision-making procedures (ISO/IEC 2005).

Enterprise security is a classical term that reflects the efforts made to avoid business risks, thus permitting a company to surpass any threat that may jeopardize its survival. The traditional concept of security needs to be expanded in order to include the aforementioned information assets, whose combination is known as Information Systems Security.

According to kluge (2008), security and information systems are therefore two closely linked terms, which is shown by the fact that any company's information is as good as the security mechanisms that are implemented over it. Unreliable information resulting from wrong security policies generates uncertainty and mistrust, and has a negative impact on every business area. Otherwise, secure information systems are a sign of certainty which contributes towards generating value both within and outside the company. Some of the current security challenges can be identified according to the innovative security approaches. These security challenges could be grouped in the following security fields: Cryptography; Security in Small and Medium Enterprises; Privacy; Security and privacy in the Cloud and Internet; Security metrics; Forensics; Security standards.

According to Doherty and Fulford (2006), enterprises have started to become conscious of the huge importance of having adequate information systems and correctly managing them, there are still many enterprises which assume the risk of having no adequate protection measures and there are many others which have understood that information systems are not useful without security management systems and the protection measures associated with them. But the implementation of these controls is not sufficient. Therefore, enterprises should use systems that manage security throughout time, thus allowing them to react to new risks,s vulnerabilities and threats that might come up.

According to NIST (2011), privacy of information is yet another challenge. From a trust perspective, it is important for enterprises to ensure that they act in a privacy conscious manner when accessing and working with an individual's personal information. The challenge now is to design pervasive computing systems that include effective privacy protection mechanisms (Bagüés, Zeidler et al., 2010). Most controls focus on information privacy as a value that is different from, but is highly interrelated with, information security. Organizations cannot have effective privacy without a solid foundation of information security. However, privacy is more than security and confidentiality, and also includes the principles of, for example, transparency, notice and choice .

1) According to Cloud Security Alliance (2009), security and privacy in the cloud and Internet. In the rush to take advantage of the benefits of Cloud computing, not least of which is the significant savings in costs, many corporations are probably rushing into Cloud computing without a serious consideration of the security implications. Although there is a significant benefit in the leverage of Cloud computing, security concerns have led organizations to hesitate at the idea of moving critical resources to the Cloud. Corporations and individuals are often concerned about how security and compliance integrity can be maintained in this new environment (Rittinghouse and Ransome, 2010).

Levels of Information Systems Security in Organizations

According to Berinato, (2005) information Systems Security is a function whose mission is to establish security policies and their associated procedures and control elements over their information assets, with the goal of guaranteeing their authenticity, confidentiality, availability and integrity. Ensuring these four characteristics is the core function of Information Systems Security in every organization.

According to Sánchez, Parra et al. (2009), authenticity allows trustful operations by guaranteeing that the handler of information is whoever he or she claims to be. Authenticity: In computing, e-Business, and information security, it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim to be. Some information security systems incorporate authentication features such as "digital signatures", which give evidence that the message data is genuine and was sent by someone possessing the proper signing key.

According to Barlette and Vladislav (2008), confidentiality is understood in the sense that only authorized users can access the information, thus avoiding this information being spread among users who do not have the proper rights.

According to Staden and Olivier (2011) availability refers to being able to access information whenever necessary, thus guaranteeing that the services offered can be used when needed.

According to Fal (2010), integrity is the quality which shows that the information has not been modified by third parties, and ensures its correctness and completeness.

a) Non-repudiation: In law, non-repudiation implies one's intention to fulfil their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction. Berinato, (2005)

The Confidentiality, Integrity, Availability (CIA) information systems security model

A simple but widely-applicable security model is the CIA triad; standing for Confidentiality, Integrity and Availability; three key principles which should be guaranteed in any kind of secure system.

According to Bobby (2008) the CIA (confidentiality, integrity, availability) principle is applicable across the whole subject of Security Analysis, from access to a user's internet history to security of encrypted data across the internet. If any one of the three can be breached it can have serious consequences for the parties concerned.

Confidentiality: Confidentiality is the ability to hide information from those people unauthorised to view it. It is perhaps the most obvious aspect of the CIA triad when it comes to security; but correspondingly, it is also the one which is attacked most often. Cryptography and Encryption methods are an example of an attempt to ensure confidentiality of data transferred from one computer to another.

Integrity is the ability to ensure that data is an accurate and unchanged representation of the original secure information. One type of security attack is to intercept some important data and make changes to it before sending it on to the intended receiver.

b) Availability is important to ensure that the information concerned is readily accessible to the authorised viewer at all times. Some types of security attack attempt to deny access to the appropriate user, either for the sake of inconveniencing them, or because there is some secondary effect. For example, by breaking the web site for a particular search engine, a rival may become more popular.

This model is a worldwide recognized model for evaluating security of information systems (Karen and Forcht, 1994) and since this study is about assessing the challenges faced by TRA in ensuring security of their information system and measuring the security level of TRAs information system, the CIA model is relevant. Specifically, TRA's information system will be evaluated along confidentiality, integrity and availability.

Review of Related Literature

A study by the Computer Security Institute and Federal Bureau of Investigation reported that approximately 90% of respondent organizations in 2001 and 2002 detected computer security breaches (Powe, 2002). Moreover, these studies found that the losses averaged over 2 million dollars per organization. In contrast, companies only spend 0.047 percent of their revenues on security [Geer 2003], and this indicates that many firms are not adequately investing in information security (Farahmand, Navathe, Sharp and Enslow, 2006)

According to the study of the Computer Crime and Security Survey (2007), conducted jointly by the Computer Security Institute and the San Francisco Office of the Federal Bureau of Investigation, 46 percent of respondents reported some form of security incident during the year 2006 (Richardson 2007). Moreover, security incidents, such as viruses, system penetrations, insider abuse, or other forms of unauthorized access continue to increase in sophistication and impact, with the average annual loss reported by U.S. companies doubling from $168,000 in 2006 to $350,424 in 2007 (Richardson 2007).

In a study by Farahmand, Navathe, Sharp and Enslow (2006) to assess Damages of Information Security Incidents and Selection of Control Measures, law enforcement agencies dealing with computer crime and with executives from financial institutions dealing with security issues were interviewed. It was discovered that, disclosure and theft of proprietary information was a major threat, Virus, Denial of Service, disgruntled employees, improper password security, hardware failures were also mentioned as threats, and unauthorized users were identified as the source of the most important threats to an organization that can be caused by software techniques. Among the techniques for overcoming these threats include: scanners for viruses, and passwords, firewalls, IDS systems for break-ins and background checks were all mentioned. Access control was also listed as the most effective control measure for a threat. Many respondents reported dissatisfaction of users on using passwords and authentication.

A study by NRC (1997) categorizes information system challenges into five levels, listed in increasing order of sophistication: Accidental disclosure: Healthcare personnel unintentionally disclose patient, Insider curiosity, Data breach by insider, Data breach by outsider with physical intrusion, Unauthorised intrusion of network system: An outsider, including former employees, Systemic Threats

A study by Appari and Eric (2010) on information systems security in the health sector, it was discovered that 99% of doctors were given overriding privileges while only 52% required overriding rights on regular basis. They also found that security mechanisms of health information systems were overridden to access 54% of patients' records. The study proposed privacy management architecture (PRIMA) that leverages artefacts such as audit logs arising from the actual clinical workflow to infer and construct new privacy protection rules. In particular, PRIMA implements a policy refinement module that periodically examines the access logs and identifies new policy rules using sophisticated data-mining techniques. These audit logs could, as well, be used by privacy officials to determine privacy violations, which in itself is a complex process and often requires merging data from disparate sources. Unfortunately, such data merging may cause potential disclosure of patients' sensitive information to the investigators. However, these logs can be used as a starting point to ascertain who could have accessed what?

In the recently-published ESG Research Report, *Security Management and Operations:* Changes on the Horizon, ESG surveyed 315 security professionals working at North America-based enterprise organizations. Respondents were asked to define the biggest security management challenges at their organizations. Not surprisingly, the top response (50%) was budget constraints (Oltsik, 2012). It was also discovered: 30% of security professionals said that the security team spends too much time reacting to problems (and not enough time with proactive security management and planning), 24%

of security professionals said that there was a lack of security skills within the IT department, 23% of security professionals said that they had too many security tools, 19% of security professionals said that their organization lacks the appropriate level of security intelligence to make accurate and timely decisions, 19% of security professionals said that there was a lack of security skills within the security team itself.

A survey by Knapp (2006), Marshall, Rainer and Morrow involved 874 CISSPs. It was aimed at establishing their level of agreement concerning the top five information systems security issues across the demographics of survey participants. With the exception of the healthcare industry, the top five rankings in the larger demographic categories as ranked by the entire sample of 874 respondents are: top management support, user awareness training & education, malware, patch management, and vulnerability & risk management. The modest variation in the rankings among the demographics is not entirely surprising considering the global nature of many cyber-threats. Yet this finding is verification that many of the top ranked issues are almost uniformly critical across key demographics.

III. METHODOLOGY

Research Design

The study employed descriptive cross sectional survey . Descriptive research design involves a process of collecting data in order to test the hypothesis or answer questions concerning the current status of the subjects in the study (Mugenda and mugenda, 2003). The researcher will employ descriptive research design by first formulating research objectives, design the method of data collection (liker scaled questionnaires), select the sample size, collect data and lastly analyze the results. Descriptive research design will assist the researcher in describing and explaining present conditions in the institutions by using many subjects to fully describe the phenomenon and it will also enable the researcher to determine and report the way thing are by describing the possible behaviors, attitudes, values and characteristics of respondents in the study.

Research Population

Research population refers to the total number of subjects of interest to the researcher and to which the study applied. The target population consisted of 36 staffs of the TRA Dar es salaam from which the sample was taken.

TABLE 1. Population of the study.

Company staffs	Population	Percentage
Managerial staffs	7	16
Non managerial	29	84
Total	36	100

Sample Size

A sample is a subset of the whole population which is actually investigated by a researcher and whose characteristics was generalized to the whole population. In order to reach a high statistical value the sample size has to be as large as possible but it has to depend also on factors like the available time, money, assistance and other forms of support. The sample size for this research is 30. It is determined by using the mathematical formula (solvent formula).

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

Where 'N' is the population, 'n' is the sample size and 'e' is 0.05 (confidence level), sample size is calculated as shown in the table below according to Ram, (2009).

TABLE 2. Sample size of the study.

Company stuffs	Population	Sample	Percentage
Managerial staffs	7	5	16
Non managerial	29	25	84
Total	**36**	**30**	**100**

Source: Ram (2009)

Sampling Procedure

A stratified random sample technique was used to select the sample size. A stratified random sample is a sample obtained by dividing the population into groups with similar characteristics called strata, thereafter, a few members of each strata are selected from which random sampling was applied. The strata included managerial stuffs and non-managerial stuffs.

Research Instrument

This study used a structured questionnaire as research instrument to collect data from the respondents. Only closed ended questions with likert scale was given to the cross section of respondents which in turn facilitated effective data gathering. The researcher adopted this type of questionnaires because questions asked in it are easy to complete, analyze quantitatively and responses obtained through the use of this kind of questionnaire can be compared easily to different items hence making it easy for the researcher to detect a trend just by glancing at the responses.

Validity and Reliability of the Instrument

Validity

Validity is the degree to which the findings correctly map the phenomenon in question. The researcher employed *face validity* and utilized the experts to examine the questionnaires to ensure facial validity and the content. Their comments and suggestions were used to revise the questionnaires before making the final one.

Reliability

The test-retest technique was used, this is one of the techniques for assessing reliability of data which involves administering the same instrument twice to the same group of subjects. The research instrument (questionnaire) was administered to the respondents after sometime between one to two weeks from the first set of administration. This follows the required procedures which include selecting appropriate respondents and administering the test to them, and finally correlating the scores from both tests to evaluate the results

Data Analysis

After data has been collected from the field, the researcher went ahead and analyze it qualitatively and statistically. Frequencies and percentage distributions was used to analyze data on the respondents profile.

Ethical Considerations

Throughout this research study, the researcher avoided everything that could cause discredit on him. The researcher did this by complying to various ethical principles For instance the principle of voluntary participation that requires people not to be coerced into participating in research were adhered to where by participants was induced to participate into the study willingly and enthusiastically without necessarily being forced by the researcher. Informed consent- where by prospective research participants was fully informed about the procedures and risks involved in research. Confidentiality- where the researcher made sure that information obtained from the respondents is kept secretly and this was even guaranteed by not even allowing them to show their identity for stance on the filled questionnaires.

Limitations of the Study

Some respondents may voluntarily refuse to respond to some questions fearing that management may victimize them. However this was minimized by the researcher via cultivating and instilling a sense of trust in the minds of respondents and assuring them confidentiality.

Difficulty in accessing the respondents due to their busy schedules; however the researcher used multiple skills like call backs, re arranging appointments and extensive mappings.

Extraneous variables which was beyond the researchers control such as respondent's honesty, personal biases and uncontrolled setting of the study are likely also to challenge researchers study.

Testing: The use of research assistants with could bring about inconsistency in the administration of the questionnaires in terms of time of administration, understanding of the items in the questionnaires and explanations given to the respondents. To minimize this threat, the research assistants was briefed on the procedures to be done in data collection.

IV. Data Analysis and Findings

TABLE 3. Demographic characteristics of the respondents.

Main category	Subcategory	Frequency	Percentage
Gender	Male	15	68
	Female	7	32
	Total	**22**	**100**
Age	20-30 years	9	40.9
	31-40 years	1	4.5
	41-50 years	5	22.7
	Above	7	31.8
	Total	**22**	**100**

Findings from the questionnaire

The TRA respondents they asked that Locks are placed on all places with important information system, 10 respondents (45.5%) agree, while 7 respondents (31.8) strong agree, 3 respondents (13.6%) are neutral, 2 respondents (9%) disagree and there is no any respondent (0%) who strongly disagree.

TRA uses usernames and password to log in to the system, 13 respondents (59%) strongly agree, while 8 respondents (36.4%) agree, 1 respondent (4.5%) is neutral and there is no any respondent who disagree or strong disagree.

TABLE 4. Techniques that can be used to secure information systems in organizations.

Statements	SA	A	N	D	SD
Locks are placed on all places with important information system	7	10	3	2	0
TRA uses usernames and password	13	8	1	0	0
Users are well trained to secure to keep systems	4	10	4	3	1
Intrusion detection systems are in place and functioning properly	3	13	4	2	0
Data backup is done regularly	5	16	1	0	0
Data encryption is done before data is sent over the network	4	13	4	0	1
Fire extinguishers are in place in case of outbreaks	12	9	1	0	0
Smoke detectors are installed in datacenters	10	11	1	0	0
Data centers are well equipped with strong walls	8	12	1	0	1
Turn style doors are used on data center entrances to control traffic	4	7	6	3	2
Security camera are installed at key areas to watch traffic	9	12	1	0	0
Id is are used to limit movement into data centers	8	10	4	0	0

TABLE 5. Data is analysed in percentage (%).

Statements	SA	A	N	D	SD
Locks are placed on all places with important information system	31.8	45.5	13.6	9	0
TRA uses usernames and password	59	36.4	4.5	0	0
Users are well trained to secure to keep systems	18.2	45.5	18.2	13.6	4.5
Intrusion detection systems are in place and functioning properly	13.6	59	18.2	9	0
Data backup is done regularly	22.8	72.7	4.5	0	0
Data encryption is done before data is sent over the network	18.2	59	18.2	0	4.5
Fire extinguishers are in place in case of outbreaks	54.5	40.9	4.5	0	0
Smoke detectors are installed in datacenters	45.5	50	4.5	0	0
Data centers are well equipped with strong walls	36.4	54.5	4.5	0	4.5
Turn style doors are used on data center entrances to control traffic	18.2	31.8	27.3	13.6	9
Security camera are installed at key areas to watch traffic	40.9	54.5	4.5	0	0
Id is are used to limit movement into data centers	36.4	45.5	18.2	0	0

TRA Users are well trained to secure to keep systems, 10 respondents (45.5%) agree, while 4 respondents (18.2%) strong agree, 4 respondents (18.2%) are neutral, 3 respondents (13.6%) disagree and 1 respondent (4.5%) strong disagree.

Intrusion detection systems are in place and functioning properly,13 respondents (59%) agree, while 4 respondents (18.2%) are neutral, 3 respondent (13.6%) strong agree, 2 respondents (9%) disagree and there is no any respondent (0%) who strong disagree.

Data backup is done regularly, 16 respondents (72.7%) agree, while 5 respondents (22.8%) strong agree, 1 respondent (4.5%) is neutral and there is no any respondent who disagree or strong disagree.

Data encryption is done before data is sent over the network, 13 respondents (59%) agree, while 4 respondents (18.2%) strong agree, 4 respondents (18.2%) are neutral,1 respondent (4.5%) strong disagree and there is no any respondent who disagree.

Fire extinguishers are in place in case of outbreaks, 12 respondents (54.5%) strong agree, while 9 respondents (40.9%) agree, 1 respondent (4.5%) is neutral and there is no any respondent who disagree or strong disagree.

Smoke detectors are installed in datacenters, 11 respondents (50%) agree, while 10 respondents (45.5%) strong agree, 1 respondent (4.5%) is neutral and there is no any respondent who disagree or strong disagree.

TRA data centers are well equipped with strong walls, 12 respondents (54.5%) agree, while 8 respondents (36.4%) strong agree, 1 respondent (4.5%) is neutral, 1 respondent (4.5%) strong disagree and there is no any respondent who disagree.

TRA uses turn style doors on data center entrances to control traffic, 7 respondents (31.8%) agree, while 6 respondents (27.3%) are neutral, 4 respondents (18.2%) agree, 3 respondents (13.6%) disagree and 2 respondents (9%) strong disagree.

Security camera are installed at key areas to watch traffic, 12 respondents (54.5%) agree, while 9 respondents (40.9%) strong agree, 1 respondent (4.5%) is neutral and there is no any respondent who disagree or strong disagree.

TRA uses Id to limit movement into data centers, 10 respondents (45.5%) agree, while 8 respondents (36.4%) strong agree, 4 respondents are neutral and there is no any respondent who disagree (0%) or strong disagree (0%).

The ever changing nature of ICT makes security a challenge, 11 respondents (50%) strong agree, while 8 respondents (36.4%) agree, 2 respondents (9%) are neutral, 1 respondent (4.5%) disagree and there is no any respondent who strongly disagree.

TABLE 6. Challenges faced by TRA in ensuring the security of its information system.

Statements	SA	A	N	D	SD
The ever changing nature of ICT makes security a challenge	11	8	2	1	0
We always suffer from virus attacks	2	6	4	9	1
Some users are trained to observe security procedures	2	16	1	2	1
Most effective security measures are costly that TRA finds them expensive to implement	4	6	5	6	1
Some users misuse the system	3	14	5	0	0
Some users share their usernames and passwords with colleagues	2	11	4	5	0
Some users use the internet to browse sites that use a lot of bandwidth	5	13	3	1	0
The IT team is not affluent on securing the system	0	5	3	12	2
You feel management does not fully support IT department	0	9	1	6	6

TRA information systems always suffer from virus attacks, 9 respondents (40.9%) disagree, while 6 respondents (27.3%) agree, 4 respondents (18.2%) are neutral, 2 respondents (9%) strongly agree and 1 respondent (4.5%) strong disagree.

Some users are trained to observe security procedures, 16 respondents (72.8%) agree, while 2 respondents (9%) strong agree, 2 respondents (9%) disagree, 1 respondent (4.5%) is neutral and 1 respondent (4.5%) strongly disagree.

TABLE 7. Data analysed in percentage (%).

Statements	SA	A	N	D	SD
1. The ever changing nature of ICT makes security a challenge	50	36.4	9	4.5	0
2. We always suffer from virus attacks	9	27.3	18.2	40.9	4.5
3. Some users are trained to observe security procedures	9	72.8	4.5	9	4.5
4. Most effective security measures are costly that TRA finds them expensive to implement	18.2	27.3	22.9	27.3	4.5
5. Some users misuse the system	13.6	63.6	22.7	0	0
6. Some users share their usernames and passwords with colleagues	9	50	18.2	22.7	0
7. Some users use the internet to browse sites that use a lot of bandwidth	22.7	59	13.6	4.5	0
8. The IT team is not affluent on securing the system	0	22.7	13.6	54.5	9
9. You feel management does not fully support IT department	0	40.9	4.5	27.3	27.3

Most effective security measures are costly that TRA finds them expensive to implement, 6 respondents (27.3%) agree, while 6 respondents (27.3%) disagree, 5 respondents (22.7%) are neutral, 4 respondents (18.2%) strongly agree and 1 respondent (4.5%) strongly disagree.

Some users misuse the system, 14 respondents (63.6%) agree, while 5 respondents (22.7%) are neutral, 3 respondents (13.6%) strongly agree and there is no any respondent who disagree or strongly disagree.

Some users share their usernames and passwords with colleagues, 11 respondents (50%) agree, while 5 respondents (22.7%) disagree, 4 respondents (18.2) are neutral, 2 respondents (9%) strongly agree and there is no any respondent who strongly disagree.

Some users use the internet to browse sites that use a lot of bandwidth, 13 respondents (59%) agree, while 5 respondents (22.7%) strongly agree, 3 respondents (13.6%) are neutral, 1 respondent (4.5%) disagree and there is no any respondent who strongly disagree.

TABLE 8. Level of information system security at TRA.

Statements	SA	A	N	D	SD
Information is only accessed by those supposed to	4	14	3	1	0
Information is only changed in the right way by the correct way	6	14	2	0	0
The system (printers and other accessories) is always available whenever they are needed	3	17	2	0	0
The hardware of the system is only accessed by the right people	3	12	6	1	0
The information on the system is always available whenever they are needed	1	17	4	0	0
The system (hardware and all accessories) are only accessed by those supposed to	3	14	3	2	0

The IT team is not affluent on securing the system, 12 respondents (54.5%) disagree, while 5 respondents (22.7%) agree, 3 respondents (13.6%) are neutral, 2 respondents (9%) are strongly disagree and there is no any respondent (0%) who strongly agree.

TRA IT staff they feel that management does not fully support IT department, 9 respondents (40.9%) agree, while 6 respondents (27.3%) disagree, 6 respondents (27.3%) strongly disagree, 1 respondent (4.5%) is neutral.

TABLE 9. Data is analyzed in percentage (%).

Statements	SA	A	N	D	SD
Information is only accessed by those supposed to	18.2	63.6	13.6	4.5	0
Information is only changed in the right way by the correct way	27.3	63.6	9	0	0
The system (printers and other accessories) is always available whenever they are needed	13.6	77.3	9	0	0
The hardware of the system is only accessed by the right people	13.6	54.5	23.7	4.5	0
The information on the system is always available whenever they are needed	4.5	77.3	18.2	0	0
The system (hardware and all accessories) are only accessed by those supposed to	13.6	63.6	13.6	9	0

Information is only accessed by those supposed to, 14 respondents (63.6%) agree, while 4 respondents (18.2%) strongly agree, 3 respondents (13.6%) are neutral, 1 respondent (4.5%) disagree.

Information is only changed in the right way by the correct way, 14 respondents (63.6%) agree, 6 respondents (27.3%) strongly agree while (0%) disagree and (0%) strongly disagree.

The system (printers and other accessories) is always available whenever they are needed, 17 respondents (77.3%) agree, 3 respondents (13.6%) strongly agree, 2 respondents (9%) are neutral, while (0%) disagree and (0%) strongly disagree.

The hardware of the system is only accessed by the right people, 12 respondents (54.5%) agree, 6 respondents (27.3%) are neutral, 3 respondents (13.6%) strongly agree, 1 respondent (4.5%) disagree, while (0%) strongly disagree.

The information on the system is always available whenever they are needed, 17 respondents (77.3%) agree, 4 respondents (18.2%) are neutral, 1 respondent (4.5%) strongly agree, while (0%) disagree and (0%) strongly disagree.

The system (hardware and all accessories) are only accessed by those supposed to, 14 respondents (63.6%) agree, 3 respondents (13.6%) strongly agree, 3 respondent (13.6%) are neutral, 2 respondents (9%) disagree while (0%) strongly disagree.

V. Conclusion and Recommendations

Conclusions

The drawn conclusions based on the research objectives. The first objective was to identify techniques that can be used to secure information systems in organizations. The objective was designed so as to find out if TRA uses most important techniques to secure information systems. According to the results from the findings, majority of respondents agreed on the questions asked, it shows that TRA uses important techniques in the process of securing information systems. According to other responses of other respondents the result shows that several of TRA IT staff were not well trained about techniques that can be used to secure information systems.

The second objective was to examine the challenges faced by TRA in ensuring the security of their information systems. According to the results from the findings, majority of respondents agreed on the questions asked it shows that TRA information systems faced security challenges. The challenges like users to misuse the system and inadequate trainings to system users to observe security procedures seems as big challenges because majority of respondents agree with these challenges and it is clear that emergence of these challenges causes occurrence of other challenges.

The third objective was to determine the level of information system security of TRA. According to the results of findings it shows that the level of information system security is high. It seems that the administration of IT department is fighting to ensure security of information system against information system security challenges of its organization.

Recommendations

It seems that TRA uses most important techniques which are used to secure Information System but still IT department is required to increase effort in the process of identifying new challenges which are increasing day to day due to the development of technology and to put consideration concerning employment of new techniques so as to ensure information system security.

It is evident that some users misuse the system which is the big internal challenge of the organization. The IT administration should be careful with its system users because the source of the challenges may be caused by insiders of the organization who are system users. There is also a need to put efforts to train many important system users to observe security procedures which will help the process of fighting against information system security challenges.

It is evident that management does not fully support IT department. TRA management should support IT department at high rate so as to stimulate the process of ensuring information system security by TRA IT administrators.

Furthermore, the IT administration is required to ensure that each system user must use his/her own user name and password to log in to the system and to keep it secretly so as to avoid the process of sharing user names and passwords which may lead to the information system security breaches.

References

[1] Appari, A. & Eric, J.M. (2010). Information security and privacy in healthcare: current state of research', Int. J. Internet and Enterprise Management, Vol. 6(4).

[2] Allen, Julia H. (2001). The CERT Guide to System and Network Security Practices. Boston, MA: Addison-Wesley. ISBN 0-201-73723-X

[3] Baguuméés, S. A., A. Zeidler, et al. (2010). "Enabling Personal Privacy for Pervasive Computing Environments." Journal of Universal Computer Science 16(3): 34

[4] Barlette, Y. and V. Vladislav. (2008). Exploring the Suitability of IS Security Management Standards for SMEs. Hawaii International Conference on System Sciences. Waikoloa, HI, USA.

[5] Bashaw, C. (2003). Computer Forensics in Today's Investigative Process. 15th FIRSTConf. Computer Security Incident Handling & Response. Ottawa

[6] Berinato, S. (2005). "A Few Good Information Security Metrics." CSO Magazine. Cloud Security Alliance (2009). Se bcurity Guidance for Critical Areas of Focus in Cloud Computing V2.1
[7] Choo, K.-K. R., R. G. Smith, et al. (2007). Future directions in technology-enabled crime: 2007-09. Research and Public Policy Series. Australian_Government, Australian Institute of Criminology. 78
[8] Dhillon, G. a. J. B. (2000). "Information System Security Management in the NewMillennium." Communications of the ACM 43(7): 125-128.
[9] Doherty, N. F. and H. Fulford (2006). "Aligning the Information Security Policy with the Strategic Information Systems Plan." Computers & Security 25(2): 55-63.
[10] Damages of Information Security Incidents and Selecting Control Measures, a Case Study Approach. Georgia Institute of Technology.
[11] Farahmand, F., Navathe, S.B., Sharp, G.P. and Enslow, P.H.(2006). Assessing
[12] Fal, A. M. (2010). "Standardization in information security management." Cybernetics and Systems Analysis 46(3): 181-184.
[13] ISO/IEC (2005). ISO/IEC 27001 Information technology - Security techniques – Informatio security management systems - Requirements
[14] ISO/IEC27001 (2005). ISO/IEC 27001, Information Technology - Security.Techniques Information security management systemys - Requirements
[15] ITU (2009). ICT Security Standards Roadmap International Telecommunication Union. Kluge, D. (2008). Formal Information Security Standards in German Medium. Enterprises. CONISAR: The Conference on Information Systems Applied Research
[16] Knapp, K.J., Marshall, T.E., Rainer, R.K. & Morrow , D.W. (2006). The TopInformation Security Issues Facing Organizations: What Can Government Do to Help.ISC journal of information systems security.
[17] Mellado, D., C. Blanco, et al. (2010). "A Systematic Review of Security Requirements Engineering." <i<="" i=""> 32: 153-165. </i
[18] Mellado, D., E. Fernández-Medina, et al. (2007). "A Common Criteria Based Security Requirements Engineering Process for the Development of Secure Information Systems." Computer Standards and Interfaces 29(2): 244 - 253.
[19] NIST (2011). Security and Privacy Controls for Federal Information Systems and. Organizations SP 800-53, National Institute of Standards and Technology.
[20] Oltsik, J. (2012). Biggest Information Security Management Challenges for Enterprises Organizations.ESG
[21] Oso & David Onen (2008). Research Guideline book. Kampala. ISBN.
[22] Rittinghouse, J. W. and J. F. Ransome, Eds. (2010). Cloud Computing Implementation, Management, and Security, CRC Press.
[23] Sánchez, L. E., A. S.-O. Parra, et al. (2009). "Managing Security and its Maturity in Small and Medium-sized Enterprises " Journal of Universal Computer Science 15(15): 3038 - 3058
[24] Staden, W. v. and M. S. Olivier (2011). "On Compound Purposes and Compound Reasons for Enabling Privacy." Journal of Universal Computer Science 17(3): 426-450.
[25] Woo-Sung Park, Sun-Won Seo, et al. (2010). "Analysis of Information Securi Management Systems at 5 Domestic Hospitals with More than 500 Beds." HIR - Healthc Inform Research: 90-99.