ACSIJ Advances in Computer Science: an International Journal, Vol. 3, Issue 3, No.9 , May 2014
ISSN : 2322-5157
www.ACSIJ.org

ACSIJ
WWW.ACSIJ.ORG

Current Status of e-Government Services in Tanzania: A Security Perspective

Mohamed Dewa[1] and Irina Zlotnikova[2]
The Nelson Mandela African Institution of Science and Technology (NM-AIST)
School of Computational and Communication Science and Engineering
P. O. Box 447, Arusha, Tanzania
Email: {dewam[1], irina.zlotnikova[2]}@nm-aist.ac.tz

Abstract

E-Government services improve efficiency in the delivery of government services, strengthen citizen participation, build trust in government, and yield cost savings for citizens, businesses and the government itself. However, the use of e-Government services depends on the citizens' trust towards security of these services. This paper assesses the current status of security in e-Government services in Tanzania. The practices which influence the security of e-Government services were identified. The collected data on security practices collected from five Tanzanian public organizations using questionnaires was processed and analyzed using the SPSS. The results indicate that e-Government services are not fully secured because the majority of organizations protect their ICT assets by implementing only technical security controls rather than complementing them with non technical security controls. We conclude that more efforts are needed to secure e-Government services by applying the activities proposed in this paper.

Keywords**:** *e-Government, e-Government services, technical security controls, security practices, security awareness*

1. Introduction

E-Government is a generic term for web-based services from agencies of local, state and federal governments [1]. In e-Government, the government uses Information and Communications Technology (ICT) and particularly the Internet to support government operations, engage citizens, and provide government services. The interaction may be in the form of obtaining information, filings, or making payments and a host of other activities via the World Wide Web [1]. E-Government services utilize ICT to transform and enhance the relationship of the public sector and its clients through an improved range and quality of service [2]. ICT can serve a variety of different purposes: (1) better delivery of government services to citizens, (2) improved interactions with business and industry, (3) citizen empowerment through access to information, or (4) more efficient government management. The resulting benefits can be less corruption, increased transparency, greater convenience, revenue growth, and/or cost reductions [3].

The government of Tanzania recognizes that by using e- Government services the government will be able to increase the range and quality of services in public sectors [4]. Various efforts have been made to deploy e-Government initiatives in Tanzania. In 2012 the government of Tanzania established the e-Government agency which is a semi-autonomous institution with the mandate of coordination, oversight and provision of e-Government initiatives and enforcement of e-Government standard in the public services [5]. The government of Tanzania also adopted an e-Government strategy (2009) that is aimed at improving efficiency in government and providing better services to citizens. Information security is identified as one of the requirements for the successful e-Government implementation although the government has not adopted any standards or issued guidelines to government agencies with regards to information security [6].

Bonham and others agree that one of the most significant barriers for implementing e-Government applications is computer security, privacy and confidentiality of the personal data [7]. According to most e-Government plans, providing services over the Internet will yield higher efficiency and quality, easier access, the possibility of offering individual services, and increased transparency, ultimately leading to a more efficient public sector [8]. As a result, there are increasing concerns about the reliability and security of the developed websites and applications, in order to ensure that services will be provided to customers with the maximum possible security, to guarantee the integrity of the system and the privacy of online users [8]. The effective management of information security is a key factor as willingness of the different users (citizens and other parties) to use e-Government services will heavily depend on the trust they have on the security of this service [9].

Some studies [10, 11] show that while most of the developed countries are in the final stages of e-government development, developing countries are still in the early stages of e-government development. This difference is heavily influenced

by the existence of technological and non-technological related issues including lack of proper ICT infrastructures, readiness, awareness, economical, and political will.

Current system development methodologies fail to effectively integrate security and systems engineering, basically because they lack concepts and models as well as a systematic approach towards security. To achieve a secured e-Government service, security requirements should be identified and considered during the whole development process of the e-Government service.

The purpose of this paper is to assess the current status of security in e-Government services in Tanzania. The paper is a part of ongoing research which aims at developing a holistic secured maturity model for protecting information in e-Government services in Tanzania.

1.1 Background

E-Government services must build trust with users (citizens, businesses and government). Citizens' trust plays a very vital role in the adoption and acceptance of e-Government initiatives [12]. Users are unlikely to use e-Government services without a guarantee of trust. The issue of trust involves several security issues. This section identifies the security requirements to e-Government services. Governmental websites and online services, however, may not require the application of all identified security requirements. Normally each service has specific requirements depending on its objectives and functionalities.

1.1.1 Confidentiality

The first issue to be considered when developing an e-Government service is privacy or confidentiality which means, protecting information from unauthorized disclosure [13]. Governments collect vast quantities of data on their citizens through everyday transactions. Protecting the privacy of citizens' personal information stored on these databases while making effective use of the information contained in them is a vitally important issue [14]. Governmental websites and online services should integrate privacy protections and should adhere to privacy best practices by educating and training officials on the importance of confidentiality.

1.1.2 Integrity

Integrity is the second issue to be considered. Integrity means, a capability to prevent information from unauthorized modification, and ensuring that information can be relied upon and is accurate and complete [9]. This means that, with integrity controls, data cannot be modified in an unauthorized or undetected manner. Integrity is violated when data/ information in transit is modified. Government websites and online services should have the ability to ensure that data cannot be altered by unauthorized user.

1.1.3 Availability

The third issue to be considered is availability. Availability means, assets/ information are accessible (available) to authorized parties at appropriate times [15]. In other words, if an authorized user (person or system) wants to access particular information, that access should not be prevented. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly [16]. Ensuring availability also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system essentially forcing it to shut down [16]. E-Government services should be available to authorized users when needed. This situation requires an organization to have business continuity and disaster recovery planning, performs hardware/ software maintenance immediately when needed, implements emergency backup power systems, periodically upgrades system, protects against malicious code and provides adequate bandwidth.

1.1.4 Non-repudiation

Non-repudiation is the forth issue to be considered. Non-repudiation means, a capability to prevent the intervening person or system in an event or action to denying or challenging their participation on the event [9]. Users of government services should be assured that the services provided are secured in such a way that no party involved in any transaction can deny his/ her participation in doing any activity to accomplish the transaction.

1.1.5 Authentication

The fifth issue to be considered is authentication which means, the process of determining whether someone or something is, in fact, who or what it is declared to be and is genuine [17]. Government websites and online services should have the capability of ensuring that the parties involved in any transaction are who they claim to be, and the data, transactions, communications or documents are genuine.

1.1.6 Authorization

Authorization is the sixth issue to be considered. Authorization means, the process of giving someone (person or system) permission to do or to

have something [17]. This implies that in order to be able to give a user access to any system's resource this user should first be authenticated. Government websites and online services should have the capability of granting specific rights to authorized users. Users should be granted rights to access only the information and resources that are necessary for their legitimate purpose.

1.1.7 Traceability

The seventh issue to be considered is traceability. Traceability means, a capability to chronologically interrelate any transaction to a person or system that performed the action in a way that is verifiable [9]. Transaction tracking can mean that each interaction with the system can be traced back to an individual user which increases accountability. Traceability controls the access of information and tracks any illegal activities. Government websites and online services should be designed to determine which information is relevant and provide proper logging infrastructure. This includes planning where and for how long log information is stored.

1.1.8 Accountability

The eighth issue to be considered is accountability which means, the use of information should be transparent so it is possible to determine whether a particular use is appropriate under a given set of rules and that the system enables individuals and institutions to be held accountable for misuse [18]. This implies a capability of linking an action to a user that can be held responsible. Government websites and online services should be designed to accommodate accountability concept whereby every user who works with an information system should have specific responsibilities for information assurance.

1.1.9 User Anonymity

The ninth issue to be considered is user anonymity which means, a capability of preventing the disclosure of information that leads to the identification of the user [19]. User anonymity is essential concept in some e-Services such as e-voting. Government websites and online services that collect information for survey purposes should be designed to support user anonymity concept.

1.1.10 Security Awareness

The tenth issue to be considered is security awareness which means, users' understanding towards the importance of information security and their responsibility to protect organization data [20]. Security awareness provides an understanding of various information technology threats that exist and taking reasonable steps to guard against them. Most organizations concentrate on technical solutions. The reality is that no technical solution alone can make information systems more secure. Non-technical solutions should be considered to protect information systems resources, because poor practices by users can easily overcome the best planned security system. Users of Government websites and online services should be aware of information security concepts by educating them and providing security awareness training periodically.

1.2 General Objective

The general objective of this study was to assess the current status of security in e-Government services in Tanzania.

1.3 Specific Objectives

The specific objectives of this study were

i. To identify the current practices of protecting information in e-Government services in Tanzania.
ii. To identify the security requirements of e-Government services in Tanzania.
iii. To recommend activities for improving security in e-Government services in Tanzania.

2. Methodology

In identifying the current practices of protecting information in e-Government services in Tanzania, data were collected using structured questionnaires which were distributed to (1) the staff with ICT skills, (2) ICT security experts, (3) the top management, and (4) the operational staff. We consulted human resource department personnel of each of the surveyed organizations to know the total number of employees and the approximate number of employees with ICT security expertise. We adopted an information security management system (ISMS) standard ISO/IEC 27001:2005 [21], which was published in October 2005 by the International Organization for Standardization (ISO) to develop the questionnaire. The desk review was conducted to identify the security requirements of e-Government services in Tanzania. Information security reference books, articles and journal papers were analyzed as a part of the extensive literature review.

2.1 Population and Sampling Method

To assess the current status of security in e-Government services in Tanzania, a population of government organizations staff was consulted. The consulted staffs were (1) the staff with ICT skills, (2) ICT security experts, (3) the top management,

and (4) the operational staff. Currently, Tanzania has 31 ministries, 17 departments, and 21 agencies. The criteria used for selection of research sample were: (1) governmental organizations which have e-Government services, and (2) governmental organizations with e-Government services which are not administered by Tanzania e-Government Agency. Based on these two criteria, five organizations were selected. Due to confidentiality reasons, we referred to them as Organizations A, B, C, D and E. Organization A is a public organization responsible for managing the overall revenue, expenditure and financing of the government. Organization B is a public organization responsible for management of public services. Organization C is a public organization responsible for managing the assessment, collection and accounting of all central government revenue. Organization D is a public organization responsible for generating, transmitting, distributing and selling electricity. Organization E is a public organization responsible for coordinating, encouraging, promoting and facilitating investment. The total population was 11,813, and the sample size of the population was estimated at 372. We distributed 400 questionnaires, and 365 responses were received.

The sample size of the population was calculated from the following formula [22]:

$$n = \frac{Z^2 \times p \times q \times N}{e^2(N-1) + Z^2 \times p \times q} \quad \text{.....} \quad (1)$$

Where N = size of population, n = size of sample, e = acceptable margin error (the precision = 0.05), Z= Z value at 95 percent confidence level (1.96), p = sample proportion, q = 1 – p; where q= 0.5.

2.2 Data Collection

Questionnaires were used to collect primary data. To ensure validity of the questionnaires, a pilot study was conducted prior distributing questionnaires to respondents. Thirty seven questionnaires were delivered to respondents, but only 12 responded. Necessary improvements to the questionnaire were done, and the improved version of the questionnaires was distributed to our sample population.

2.3 Reliability and Goodness of Fit Measurement.

The analysis of the internal consistence of the questions was conducted by doing a reliability test by using Statistical Package for Social Sciences (SPSS). The calculated Cronbach's alpha was 0.848 and thus was found suitable. To assess goodness of fit for all, survey questions, a Chi-square test was conducted and the results show statistical significance.

2.4 Data Processing and Analysis

The content analysis technique was used for processing and analyzing descriptive data. SPSS and Microsoft Excel were used for data analysis. The results were presented using chats.

3. Results and Discussions

3.1 The current practices of protecting information in e-Government services in Tanzania

This study assessed the current status of security in e-Government services in Tanzania. This was done through identification and analysis of the current practices implemented for protecting information in e-Government services. The presence of the following practices influences the security of e-Government services provided by public organizations: (1) ICT security policy; (2) ICT security awareness and training programs; (3) backup mechanisms of critical information; (4) Business Continuity Plan and Disaster Recovery; (5) skilled ICT security personnel; (6) adequate bandwidth; (7) access control; (8) system application logs management; (9) technical security controls. We received 365 responses, and these responses were processed and analyzed by using the Statistical Package for Social Sciences.

3.1.1 ICT Security Policy

The analysis of the collected data shows that 70.1 percent of government organizations have ICT security policies, while 29.9 percent of organizations have no security policy. This result shows that approximately 30 percent of e-Government services are implemented without the clear explanations of how security controls should be implemented and enforced. More efforts are needed to reduce this weakness. Therefore, we recommend the establishment of a national level policy used as the guidance to all organizations. Figure 1 shows the respondents' responses on ICT security policy.

3.1.2 ICT Security Awareness and Training Programmes

We also collected and analyzed the data on ICT security awareness. It has been noted that the majority of the organizations (47.9 percent) have no security awareness training programmes, 22.7 percent of the organizations have planned

awareness programmes, while the remaining organizations (29.3 percent) conduct security awareness programs when an incident of insecurity

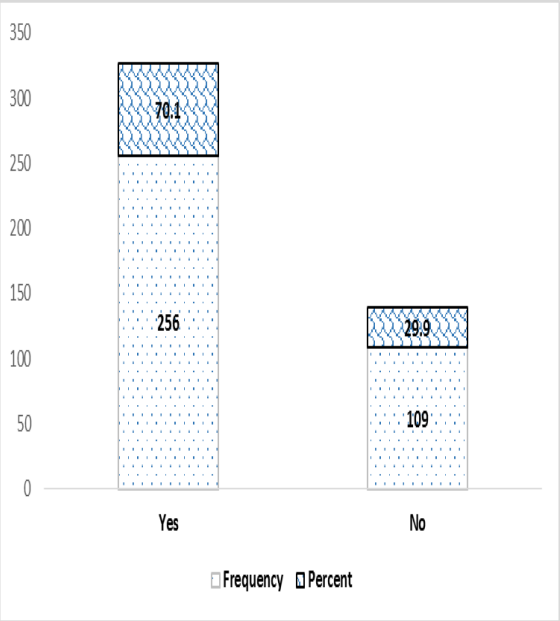

Fig. 1: Respondents' responses on ICT security policy

has occurred. This indicator shows that most of the surveyed organizations ignore security awareness training for their staff; this situation affects the users' understanding towards the importance of information security and their responsibility to protect the organization's ICT assets negatively, and hence reduce the security stability of the organization. Therefore, we recommend organizations to promote the security awareness by conducting seminars, workshops and training programmes periodically. Figure 2 shows the respondents' responses on ICT security awareness.

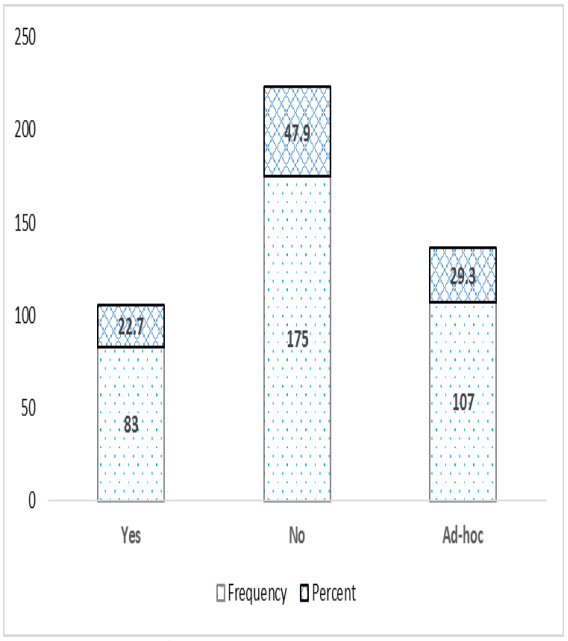

Fig. 2: Respondents' responses on ICT security awareness

3.1.3 Backup Mechanisms of Critical Information

The majority of the surveyed organizations (68.8 percent) perform backup mechanisms of their critical information periodically. However, it was noted that approximately 75 percent of these organizations do not test the restoration of the data from the backup tapes. This implies that in case of system failure 51.6 percent of organizations may not be able to restore their critical information, and hence the organizations will not be able to continue with their operations, which means unavailability of services in these organizations. Therefore, we recommend the implementation of both backup mechanisms and the restoration test of the data from the backup tapes. This ensures that both the tapes and backup procedures work properly and hence preserve the availability of sensitive data of organization. Figure 3 shows the respondents' responses on backup mechanism implementation.

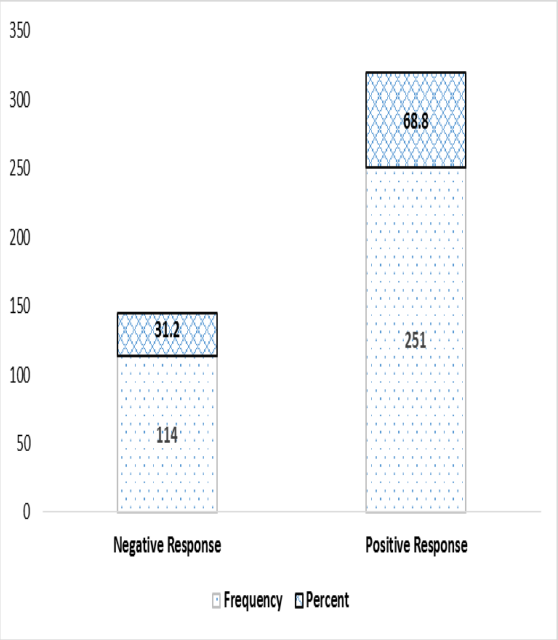

Fig. 3: Respondents' responses on backup mechanism implementation

3.1.4 Business Continuity Plan and Disaster Recovery (BCP)

We also analyzed the presence of business continuity plan and disaster recovery. The analysis shows that the majority of organizations (87.7 percent) have BCP. This implies that 12.3 percent of organizations cannot counteract interruptions to business activities to protect critical business processes from the effects of major failure of information systems or disasters to ensure their timely resumption. Thus, we recommend to the organizations which do not have BCP to have the plan. Figure 4 shows the respondents' responses on BCP.

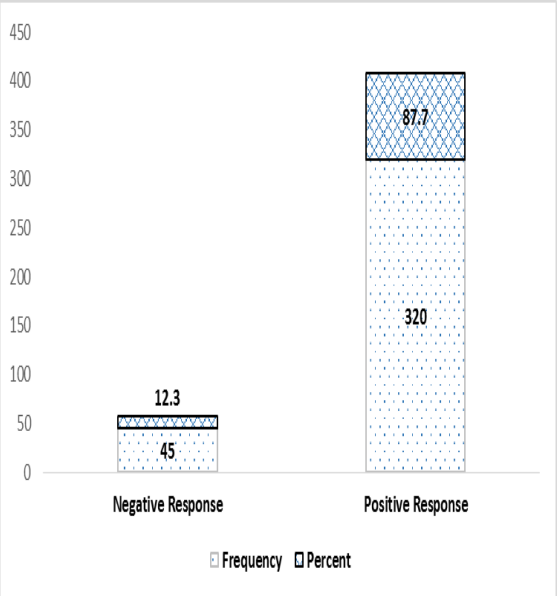

Fig. 4: Respondents' responses on BCP

3.1.5 Skilled ICT Security Personnel

The analysis of the collected data from the human resource management departments of the surveyed organizations shows that only 0.3 percent of organization personnel are ICT security skilled. This means that only 0.3 percent of personnel in government organizations have skills of planning, implementing and monitoring ICT security programs. This indicator shows that most of public organizations are incapable of initiating and implementing security programs using their in-house human resources. Therefore, we recommend government to take serious initiatives to increase the number of ICT security skilled personnel by training the available ICT related personnel to acquire security skills and employing more ICT security personnel. We can conclude that the security stability of e-Government services cannot be obtained unless organizations have sufficient ICT security skilled personnel.

3.1.6 Adequate Bandwidth Capacity

The analysis of the collected data shows that only 23.3 percent of government organizations have adequate bandwidth capacity and 76.7 percent of the organizations are not satisfied with the current bandwidth capacity. The implication of this situation is that there is a continuous delay in responding requests of e-Government service users. This situation is against the availability of ICT assets to authorized users. Thus, we recommend all public organizations to allocate a reasonable budget which enable them to acquire a satisfactory bandwidth capacity which improves the speed of e-Government services delivery. Figure 5 shows the respondents' responses on bandwidth capacity satisfaction.

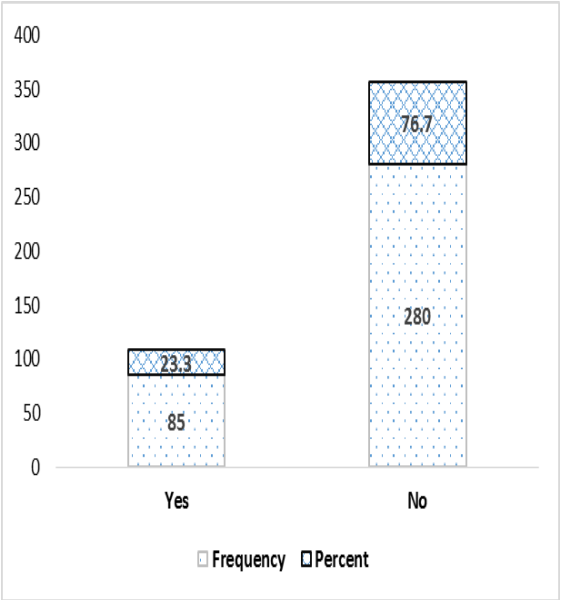

Fig. 5: Respondents' responses on bandwidth capacity satisfaction

3.1.7 Access Control

The analysis of collected data shows that 88.2 percent of surveyed organizations implement access control to enforce separation of duty. This implies that 11.8 percent of surveyed organizations are incapable of reducing risks of unauthorized users getting access to their ICT assets. This situation can lead to the bleach of confidentiality. Thus, we recommend all organizations to implement access control mechanisms to preserve confidentiality of information. We can conclude that users of e-Government services should be granted rights to access only ICT assets that are necessary for their legitimate purpose. Figure 6 shows the respondents' responses on implementation of access control mechanisms to enforce separation of duties.

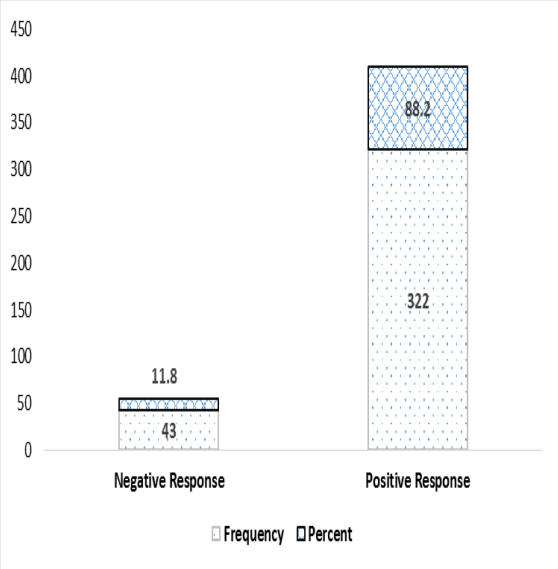

Fig. 6: Respondents' responses on implementation of access control mechanisms to enforce separation of duties.

3.1.8 System Application Logs Management

The analysis of the collected data shows that 58.1 percent of surveyed government organizations implement the management of system application logs to detect unauthorized information processing activities. However, it was noted that approximately 31 percent of these organizations do not review the results of monitored activities regularly. This implies that, in case of any late detection of unauthorized information processing activities, 59.9 percent of organizations may not be able to trace who is responsible to those unauthorized activities. Thus, we recommend all organizations to implement and review the results of monitored activities stored in the system application logs regularly. These two activities preserve the traceability and accountability properties of information security. Figure 7 shows the respondents' responses on management of system application logs.

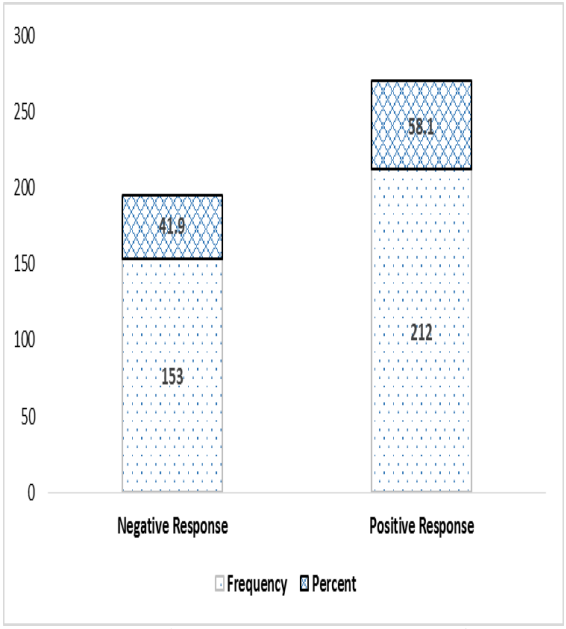

Fig. 7: Respondents' responses on management of system application logs.

3.1.9 Technical Security Controls

The analysis of the collected data shows the following:

1. The majority of organizations (96.1 percent) use antivirus software as computer viruses detective and preventive control, but it was noted that 23 percent of organizations out of this 96 percent have no updated antivirus software.
2. The majority of organizations (63.4 percent) use firewalls as their preventive control. It was noted that a number of staff use their own modems while in office, this makes the possibility of intruders or hackers to circumvent the installed firewalls.
3. The majority of organizations (58.7 percent) use Intrusion Detection Systems (IDS) as detective control and Intrusion Prevention Systems (IPS) as preventive control.
4. The minority of organizations (32.9 percent) use encrypted communication channels to preserve confidentiality of information transmitted between two points

The above indicators show that the majority of organizations make more efforts of protecting ICT assets in e-Government services by implementing technical security controls rather than complimenting them with non technical security controls. The ICT assets cannot be protected by only technical security controls, therefore, both technical and non technical security controls should be considered to protect ICT assets achieve the secured e-Government services.

4. Recommendations

Based on the findings from this study, we recommend the following activities to be done in order to improve security of e-Government services in the country:

1. Since a number of organizations (29.9 percent) have no ICT security policy, therefore, we recommend the establishment of a standard ICT policy at the national level. The presence of the national ICT security policy facilitates the information security infrastructure (laws, regulations and policies) which are not available today.
2. The level of security awareness in organizations is very low (22.7 percent), we therefore recommend organizations to promote the security awareness by conducting training programmes periodically. These awareness training should be attended by everyone in the organization who uses ICT assets. Each participant should be trained on how to keep his or her ICT assets secure to ensure a safe working environment.
3. A number of organizations (31.2 percent) do not perform backup procedures for their sensitive information. Therefore, we recommend organizations to implement both backup mechanisms and restoration test of the data from the backup tapes.
4. The result shows that 12.3 percent of organizations have no Business Continuity Plan. Therefore, we recommend organizations to establish both a Business Continuity Plan and a Disaster Recovery.
5. It was observed that the majority of organizations suffer from inadequate number of skilled and experienced ICT security personnel. We recommend government to take serious initiatives to increase the number of ICT security skilled personnel by training the available ICT related personnel to have security skills and employing more ICT security personnel.
6. The majority of the organizations are not satisfied with the current bandwidth capacity (only 23.3 percent of organizations are satisfied). We therefore recommend all public organizations to allocate a reasonable budget which enable organizations to acquire a satisfactory bandwidth capacity which improves the speed of e-Government services delivery.
7. The result shows that 11.8 percent of organizations do not implement access control mechanisms, we therefore recommend all organization to implement access control mechanisms to preserve confidentiality of information.
8. The results show that 41.9 percent of organizations do not implement system application logs, and approximately 31 percent of organizations which implement system applications logs do not review the results of monitored activities stored in the system application logs, we recommend all organizations to implement and review the results of monitored activities stored in the system application logs regularly.
9. The results show that the majority of organizations make more efforts of protecting ICT assets in e-Government services by implementing technical security controls rather than complimenting with non technical security controls, therefore, we recommend organizations to protect their ICT assets by using both technical and non technical security controls in order to achieve the secured e-Government services.

5. Conclusions

This study has assessed the current status of security in e-Government services in Tanzania. The information security practices which influence the e-Government services were identified and analyzed. The identified factors include the followings: ICT security policy, ICT security awareness and training programs, backup mechanisms of critical information, Business Continuity Plan and Disaster Recovery, skilled ICT security personnel, adequate bandwidth, access control, system application logs management and technical security controls. Data were collected through questionnaires, processed and analyzed using the SPSS software. The overall results obtained show that the governmental organizations implement only an average of 55.9 percent of security practices. We therefore conclude that the current status of e-government services are not well secured because the majority of organizations have no planned security practices implementation. Thus, more efforts are needed to secure e-Government services.

Further research work entail the development of a secured e-Government maturity model framework for protecting information in e-Government services in Tanzania.

References

[1] S. C. J. Palvia and S. S. Sharma, "E-government and e-governance: definitions/domain framework and status around the world," in *International Conference on E-governance*, 2007.

[2] J. J. Yonazi, "Enhancing adoption of e-Government initiatives in Tanzania," University of Groningen, 2010.

[3] Z. Fang, "E-government in digital era: concept, practice, and development," *International journal of the Computer, the Internet and management*, vol. 10, pp. 1-22, 2002.

[4] "Tanzania e-Government Strategy, President's Office - Public Service Management," ed, 2012.
[5] "Presidents Office, Public Service Management, Strategic Intent 2012/13 - 2016/17 e-Government Agency ", ed, 2012.
[6] C. K. Wangwe, M. M. Eloff, and L. Venter, "A sustainable information security framework for e-Government–case of Tanzania," *Technological and Economic Development of Economy*, vol. 18, pp. 117-131, 2012.
[7] G. M. Bonham, J. W. Seifert, and S. J. Thorson, "The transformational potential of e-government: the role of political leadership," 2001.
[8] R. Alshboul, "Security and Vulnerability in the E-Government Society," *Contemporary Engineering Sciences*, pp. 215-226, 2012.
[9] C. E. Jiménez, F. Falcone, J. Feng, H. Puyosa, A. Solanas, and F. González, "e-Government: Security Threats," *e-Government*, vol. 11, p. 21, 2012.
[10] S. Basu, " E-government and developing countries: an overview," *International Review of Law, Computers & Technology*, vol. 18, pp. 109-132, 2004.
[11] V. Ndou, "E-government for developing countries: opportunities and challenges," *The Electronic Journal of Information Systems in Developing Countries*, vol. 18, 2004.
[12] S. C. Srivastava and T. S. Teo, "A framework for electronic government: evolution, enablers and resource drainers," in *Proceedings of the Eighth Pacific Asia Conference on Information Systems*, 2004.
[13] S. Singh and D. S. Karaulia, "E-Governance: Information Security Issues," in *International Conference on Computer Science and Information Technology (ICCSIT'2011) Pattaya*, 2011, pp. 120-124.
[14] R. Reffat, "Developing a successful e-government," in *Symposium on e-Government: Opportunities and Challenge. Muscat Municipality, Oman*, 2003.
[15] G. K. Saha, "Software-based computing security and fault tolerance," *Ubiquity*, vol. 2004, pp. 2-2, 2004.
[16] F. Sattarova and T.-H. Kim, "IT security review: Privacy, protection, access control, assurance and system security," *International Journal of Multimedia and Ubiquitous Engineering*, vol. 2, pp. 17-32, 2007.
[17] T. Halonen, "Authentication and authorization in mobile environment," in *Tik-110.501 Seminar on Network Security*, 2000.
[18] D. J. Weitzner, H. Abelson, T. Berners-Lee, J. Feigenbaum, J. Hendler, and G. J. Sussman, "Information accountability," *Communications of the ACM*, vol. 51, pp. 82-87, 2008.
[19] M. Mehta, S. Singh, and Y. Lee, "Security in E-Services and Applications," *Network Security: Current Status and Future Directions, Edited by Douligeris C. & Serpanos DN, John Wiley & Sons*, pp. 157-178, 2007.
[20] R. S. Shaw, C. C. Chen, A. L. Harris, and H.-J. Huang, "The impact of information richness on information security awareness training effectiveness," *Computers & Education*, vol. 52, pp. 92-100, 2009.
[21] D. Mellado, E. Fernández-Medina, and M. Piattini, "A common criteria based security requirements engineering process for the development of secure information systems," *Computer standards & interfaces*, vol. 29, pp. 244-253, 2007.
[22] C. Kothari, *Research methodology: methods and techniques*: New Age International, 2004.

Authors Biographies

Mohamed D. Waziri[1] is a doctoral student at the Nelson Mandela African Institution of Science and Technology. He holds a M.Sc. Computer Science from the University of Khartoum (2007). He also holds a B.Sc. in Computer Science from the International University of Africa (2003). Mr. Waziri is currently employed at the University of Dodoma (UDOM) as Assistant Lecturer. Prior to joining UDOM he was working as Assistant Lecturer at the International University of Africa, Khartoum, Sudan.

Prof. Irina Zlotnikova[2] holds a PhD in Theory and Methodology of Computer Science Education (Doctor of Pedagogical Sciences, Moscow, Russia, 2005), a PhD in Solid-State Electronics, Nano-and Microelectronics (Candidate of Technical Sciences, Voronezh, Russia, 1995) and an Engineering Degree in Radiophysics and Electronics (Voronezh, Russia, 1988). She is a Professor of School of Computational and Communication Science and Engineering at the Nelson Mandela African Institution of Science and Technology, Arusha, Tanzania.