The International Journal of Multi-Disciplinary Research
ISSN: 3471-7102, ISBN: 978-9982-70-318-5

A Critical Review of Cybersecurity Readiness of e-Governance in Developing Countries – A Case of Zambia

(Conference ID: CFP/825/2018)

Chisanga Kapinda,
Senior ICT Security Officer – SMART Zambia Institute,
Student – Information and Communications University.
chisangakapinda@gmail.com
Lusaka, Zambia.

Abstract

Electronic Governance (e-Governance) systems are being implemented around the world to improve convenience, reduce time, improve transparency, effectiveness, efficiency and quality in delivering public services to businesses and citizens. E-Governance services are becoming one of the most important and efficient means. However, this has brought not only enormous opportunities but also serious Cybersecurity challenges. Cybersecurity is vital for the successful adoption of e-governance systems hence this paper presents an assessment of Cybersecurity readiness in government institutions towards e-governance in Zambia. This paper highlights the findings of the survey study carried out to realize the perceptions of Cybersecurity in government Institutions in Zambia. With the aid of an online survey, about 30 ICT personnel from government Institutions were surveyed about the effectiveness of Cybersecurity implementation in their Institutions. The questions were asked on information security practices such as information security policies, audits, risk management, business continuity and disaster recovery, access controls, training and awareness, qualified personnel and technologies for protection of e-governance infrastructure. The survey results show that less than 50% of respondents believed that the Cybersecurity implementation was effective with regards to such practices. The findings suggest that many of the Cybersecurity practices are inadequately implemented and therefore, there exist a serious gap in achieving a required Cybersecurity posture towards e-governance. This study recommended that government Institutions constituted comprehensive Cybersecurity programs with emphasis on information security policy, risk management, awareness and training and professional capacity building in Cybersecurity. In addition, the research study has applicable implications to both government and private Institutions for implementing and managing Cybersecurity.

Keywords: Cybersecurity, e-Governance, Government Institutions, ICT, e-services.

1. Introduction

Cybersecurity is not yet at the core of many national technology strategies especially in most developing countries (James, 2017). E-governance and Cybersecurity initiatives are in their immature stage especially in developing countries including Zambia. Therefore, implementation of both Cybersecurity and e-governance in developing countries still face more difficulties, leading to a larger failure ratio than developed countries. Cybersecurity is vital for the successful adoption of e-governance systems as Governments are increasingly reliant on the information stored and transmitted over advanced communication networks and therefore, a secure e-government of a country with strategic e-services cannot endure without effective Cybersecurity practices by host government Institutions (Serianu, 2016).

There are always several related success and failure factors associated with both Cybersecurity and e-governance and at the abstract level Cybersecurity threats posed to e-governance services could result from technical and or non-technical related issues. Technical security aspects may include vulnerability caused by poor system design, development, implementation, configuration, integration, and maintenance. Similarly, non-technical security aspects may result from lack of ethical and cultural norms, legal and contractual documents, administrative and managerial policies, operational and procedural guidelines, and awareness programs (Zhao, 2015).

Analysis of the reasons behind success and failure of Cybersecurity and e-governance is still an interesting domain of investigation hence the need for this study. This paper presents a critical review of Cybersecurity readiness in government institutions towards e-governance in Zambia. The study will through an online assessment of government institution’s Cybersecurity readiness highlight some of these factors and make recommendations on effective Cybersecurity practices towards e-governance.

The Cybersecurity categories of assessment in the survey includes information security practices such as information security policies, IT audits, business continuity and disaster recovery planning, training and awareness, security or audit personnel and technologies for protection of e-governance infrastructure. Selection of these categories, are guided by the ISO 27001 Standard, and NIST’s Guide for Assessing the Security of Controls in Federal Information Systems and Organizations. These frameworks are implemented worldwide as security standards for Cybersecurity management (ISO, 2017). The primary obstacle of the study is that Cybersecurity is a sensitive issue, whether from a private sector or a government perspective. Admission of vulnerabilities is usually seen as a weakness. This is a barrier to the discussion and inter dependency of objective information and best practices.

1.1 Research Motivation and Problem Area

Zambia and other developing countries have continued to lag not only economically but also in the implementation of Information and Communications Technologies (ICTs) in their governance systems. The identification of the factors that affect the success of e-governance in Zambia and other developing countries compared to developed countries is intended to help researchers come up with explicit answers to this problem. As one of the many factors, poor Cybersecurity implementation is of great concern towards successful e-governance (James, 2017).

Many researches have been conducted on the topic of e-governance implementation in Zambia and other developing countries but very few or none have been conducted specifically on the Cybersecurity challenges relating to e-governance. It is therefore against this background that the author sought to carry out a research to determine Cybersecurity practices such as information security policies, audits, business continuity and disaster recovery planning, training and awareness, qualified personnel and technologies for protection of e-governance infrastructure. Lastly, the author who has served as a Cybersecurity Officer in government felt that the study would be a contribution to the improvement of Cybersecurity practices in government institutions once the weaknesses had been identified by the study.

1.2 Research Goal and Research Objectives

1.2.1 Research Goal

The goal of this research work is to establish the effectiveness of Cybersecurity towards e-governance in Zambia.

1.2.2 Research Objectives

The explicit objectives being:

i. to identify the effectiveness of Cybersecurity practices in Government Institutions in Zambia;

ii. to identify ways of improving Cybersecurity in Government Institutions.

2. Literature Review

Literature review is the analysis of the book or manuscripts that researchers consulted in understanding and investigating the problem during the research (Labaree, 2009). This chapter presents a review on the subject under review. It presents the theoretical framework and comparative analysis drawn from similar surveys from a global perspective, other developing countries and the Zambian situation.

2.1 Studies Related to Cybersecurity and e-Governance

2.1.1 Africa

With regards to Cybersecurity research in developing countries, The Africa Cyber Security Report of 2016 was researched, analyzed, compiled and published by the Serianu Cyber Threat Intelligence Team in partnership with the USIU's Centre for Informatics Research and Innovation (CIRI), at the School of Science and Technology (Serianu, 2016). The report focused on four main countries – Kenya, Nigeria Ghana and Tanzania – representing East and West Africa, but also touched on a dozen other countries focusing on understanding how Cybersecurity professionals in those countries deal with specific challenges. The report identified among other issues that: -

- In just four (4) years since Serianu published its first Cybersecurity report, internet users across Africa had doubled from 167.3m people in 2012 to 448m as at June 2016. The survey established that Many of the users, mostly customers and employees had little knowledge of the level of risk they were exposing both themselves and the organizations they deal with online.
- A common theme highlighted in the report was the lack of awareness for users and limited Cybersecurity visibility for service providers. While there are high levels of investment in technologies and automation across governments and the private sector, the study found that there was no matching investment in Cyber threat prevention tools. A majority of the organizations surveyed did not have clear visibility on the Cybersecurity issues they needed to watch out for.
- Lack of practical regulatory guidance from industry regulators and government was leading to poorly implemented and unenforceable security controls since they are not local focused and instead are copied and pasted regulations.
- Using the data from leading research firms and other sources, the report estimated that the ICT security expenditure in African countries would grow from approximately USD $1.24 billion in 2015 to USD $3.6 billion in 2020. Based on the research findings most African organizations were ill-equipped and unprepared to respond to information security threats. Although there are different

initiatives in place set out to address information security issues in Africa, these initiatives cannot adequately address the current security issues. The report recommended that African and developing countries needed to focus on six (6) areas which are: -

1. Harden Public and Private ICT Infrastructure and Services
2. Enhance ICT Security Competencies
3. Cultivate Vibrant ICT Security Ecosystem
4. Increase International Collaboration
5. Government Policies
6. Eco System Engagement

2.1.2 Asia

From September to November 2014 Deloitte performed its first "information security survey" in Central Asia to better understand the current state of information security programs and governance structures of organizations in the region (Deloitte, 2014). The survey covered various industries and addressed how organizations view, formulate, implement and maintain their information security programs. The survey identified the five most relevant conclusions on the current state of information security program in Central Asia, as follows: -

1. Majority of companies had not been exposed to Cybersecurity incidents.
2. Information security policies, procedures and responsibilities were mostly in place and defined.
3. Insufficient controls to ensure third parties comply with appropriate security standards.
4. Awareness of business management and end-user around Cybersecurity risks was insufficient.
5. Though basic security measures were in place more advanced solutions were uncommon.

In 2009, the International Telecommunication Union (ITU) conducted an assessment of Computer Incident Response Team (CIRT) covering Bhutan, Bangladesh and India (ITU, 2009). The main purpose of the study was to understand and gain knowledge on how these countries were managing and responding to Cyber incidents. The study's focus was on understanding Cybersecurity challenges facing these countries and measures taken to respond to these challenges, especially establishment of CIRT to respond, coordinate and share information related to Cyber incidents.

2.1.3 Europe

From a developed world perspective, a Cybersecurity breach survey was done by Ipsos MORI, in partnership with the Institute for Criminal Justice Studies at the University of Portsmouth (Ipsos, 2018). The report detailed the findings from a quantitative and qualitative survey with UK businesses on Cybersecurity. The Department for Culture, Media and Sport (DCMS) commissioned the survey as part of the National Cyber Security Program, following a previous comparable study by the Department published in 2016.

The 2017 survey highlighted that virtually all UK businesses covered by the survey were exposed to Cybersecurity risks (Ipsos, 2017). Since 2016, the proportion with websites (85%) or social media pages (59%) had risen by 8 and 9 percentage points respectively, as has the use of cloud services (from 49% to 59%).

The 2018 survey also established that 61% held personal data on their customers electronically. In this context, 74% of UK businesses said that Cybersecurity was a high priority for their senior management, with 31% saying it was a very high priority. The proportion noting it was a very low priority lower than in 2016 (down from 13% to just 7%) – a change mainly seen among the micro and small business population.

2.1.4 Zambian Situation

Just like many other countries in the Sub-Saharan Africa, Zambia's government has the desire to implement e-government to reach to its people with a view to promote e-participation and e-consultation in the decision-making process with its citizens (Bwalya, 2009).

The Zambian government has recently made progress towards e-governance. This follows the formation of the Center of Excellence for E-government and ICT (CEEGICT) in 2015, which later changed its name to SMART Zambia Institute (SZI) in 2017. This initiative called for a Zambia transformed into information and knowledge based society supported by increased access to ICTs by all citizens by 2030 (MOF, 2015). Achieving this vision would require effective and efficient coordination of ICT interventions across the Public Service. Government had identified the need to establish an ICT Center of Excellence as key in the realization of its vision (MOF, 2015).

Other efforts have been made through the recent establishment of the Zambia National Data Center (ZNDC) infrastructures to supplement the capacity of the CEEGICT (SZI) (MTC, 2017). Despite this effort, the country still faces Cybersecurity risks due to weak Cybersecurity practices in majority government institutions that are part of e-governance structure. In the recent years it had been observed that Zambia had generally poor utilization of ICTs coupled with inadequate and untrained human resource in specialized ICTs especially in Cybersecurity. Due to this the country, had continued to rely heavily on outsource expertise and consultation for most e-governance implementation (Panos, 2011).

Earlier, the Zambian government had also resolved to develop and launch the national ICT policy which incorporates computer technology (Habeenzu, 2010). However, such a move was faced with lack of clear implementation framework and strategy seen to be seriously affecting government's efforts in developing concrete programs for turning the policy into reality.

2.2 Cybersecurity Categories Used in the Study

This assessment used five (5) security categories, with the exclusion of the systems development life cycle (SDLC), which the author found less applicable to the study.

1) Security and ICT Policy;
2) IT Audits;
3) Access Control Management and Secure Infrastructure;
4) Awareness and Training; and
5) Business Continuity and Disaster Recovery Planning.

Selection of these Cybersecurity categories are guided by the ISO 27001 Standard, and NIST's Guide for Assessing the Security of Controls in Federal Information Systems and Organizations. These frameworks are implemented worldwide as security standards for Cybersecurity management. They are based on risk management methodology and involves the use of security controls for protecting and preventing security risks (ISO, 2017). Other questions used in the study include respondents' knowledge of e-governance and outsourcing practices.

2.3 Theoretical Framework/Model

From the review, a theoretical framework on Cybersecurity and e-governance in developing Countries like Zambia includes: -

- Lack of Cybersecurity Strategies/Policies and legal & regulatory framework
- Inadequate fund allocation to Cybersecurity ecosystems
- Lack of information security awareness and persistent information security culture
- Inadequate standards and maturity models for Cybersecurity
- Lack of basic awareness, information security professionals and skills within government body
- Lack of specific sector policies
- Resistance to change, especially in public sector
- Reliance on imported hardware and software
- Lack of sector-specific R&D programs
- Lack of appropriate national and global organizational structure to deal with Cyber incidents

2.4 Personal Critique of Literature Review

Despite increased research interest on e-Governance across the globe, existing research has not adequately addressed Cybersecurity factors that affect implementation and integration of e-governance systems specifically in Zambia. Similarly, there has not been any research on the relationship of Cybersecurity and e-governance in Zambia. Despite surveys having been conducted in other developing countries on Cybersecurity, it is very difficult to generalize to the Zambian situation.

3. METHODOLOGY

With this study, the author wishes to assess Cybersecurity readiness of a country towards e-governance. The question of how to assess the Cybersecurity readiness of a country's public institutions is a sensitive issue hence the need for a methodology and approach that greatly acknowledges ethical consideration. The author has selected the exploratory case study to support the research because by a preliminary literature research, scarcely any academic works could be identified that deal with a Cybersecurity assessment in the Country of interest. Therefore, it can be assumed that not much theory exists and that is why an explorative research approach was being used in this case study methodology. To achieve the goal and objectives of the study, the author would borrow a framework of information security management to derive security categories that would be used to answer specific questions from the objectives. The questions would be asked to participants through online forms. The results would be analyzed for the security categories they associated with. The adopted methodology for this study was mixed research which was mainly qualitative.

3.1 Project Design / Approach

Given the nature of this research work, it was imperative to identify and apply suitable research approaches that are well structured, comprehensive and elaborate. As a result, a generic research onion process, was adopted to guide this research work.

The process has the following layers: research philosophies and research approaches, research methods and strategies, and data collection and analysis techniques. What follows is the description of how these research layers were applied in this research work. Additionally, outlines of the research sample selections, ethical issues, are given.

The survey questionnaire was designed to cover different aspects of Cybersecurity categories discussed earlier. Questions were framed cautiously to make them easy to understand and avoid biases of respondents. Those design processes ensure that the questions meet the national and University quality and ethical standards, and that questions are well organized including the length of the survey. Furthermore, the questionnaire provided for anonymity for the respondents and their organizations as a way to promote more objectivity in their responses.

3.2 Sampling Procedure

The study environment of this research work was within the public sector consisting of only government Institutions. To successfully gather the needed data, the researcher employed mainly purposive technique. This was ideal seeing that in the technique, the researcher chooses the sample based on who would be appropriate for the study and in the case of the study, one ICT professional would give a fairly accurate perception of an organization. The main objective of purposive sampling is to arrive at a sample that can adequately answer the research objectives and in the case of this study were mainly ICT Personnel who had knowledge about their organization. The researcher would have a purposive sample accomplished by applying expert knowledge of the target population to select in a non-random manner a sample to represent a cross section of population (Lavrakas, 2008).

3.3 Target Population and Sample Size

The targeted study population was thirty (30) ICT professionals in randomly selected government Ministries and Departments. The Institutions are actively or at least passively involved in the implementation of e-governance or provision of supporting ICT Infrastructure hence the selection. The survey was not limited to their Headquarters within Lusaka by nature of being an online survey. Therefore, ICT personnel in other locations countrywide participated.

3.4 Research Data Collection, Processing and Analysis Techniques

The mechanisms employed in data collection included the use of both online questionnaires and interviews with a few participants the author interacted with. The online questionnaires were preferred in this study because of the convenience on both the author and respondents. The data was encoded and analyzed using descriptive statistics such as, percentages and figures. Statistics/Data Analysis (STATA) was used to analyze the data.

3.5 Ethical Issues Considerations

Ethics is an important issue when conducting research (Sagepub, 2007). This research work was guided by the practical principles cited by Sagepub. Plagiarism was avoided by acknowledging all used sources by referencing. Also, confidentiality of the collected data from the studied organizations was ensured by providing anonymity to both respondents and their specific organizations. Further, the study subjectivity was avoided during the data collection, processing and analysis, and reporting the final research results by the use of automated presentation such as google summery graphs. The graphs represented responses from respondents directly from the questions in percentages.

To help in carrying out the research, the author sought for a letter of introduction from the Information Communication University Registrar ‘s office.

4. RESULTS AND FINDINGS

4.1. Results / Research findings

4.1.1 Key Findings /Cybersecurity Readiness for e-Governance

The study used descriptive statistics to analyze the survey results. A frequency distribution for each question item has been calculated and aggregated into various Cybersecurity management practices. The findings from the survey results from 22 out of the targeted 30 respondents are illustrated by Figures 1 to 13 as follows: -

Figure 1. Respondents Roles

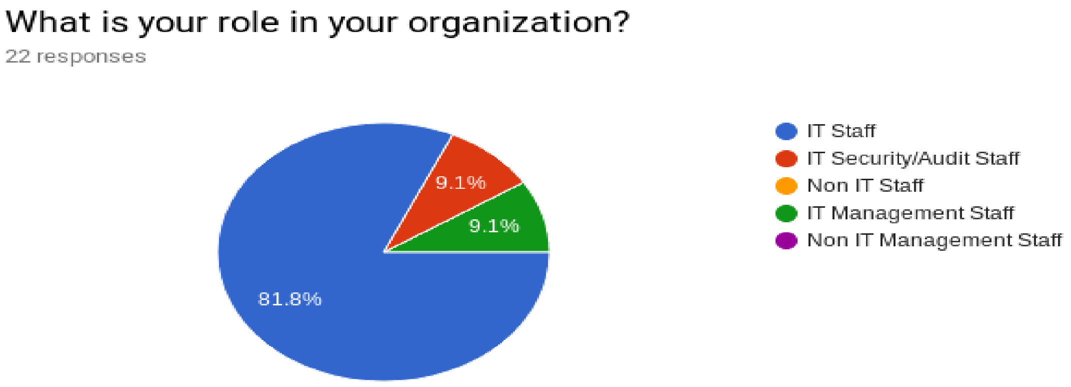


Figure 2. Organizations providing e-services

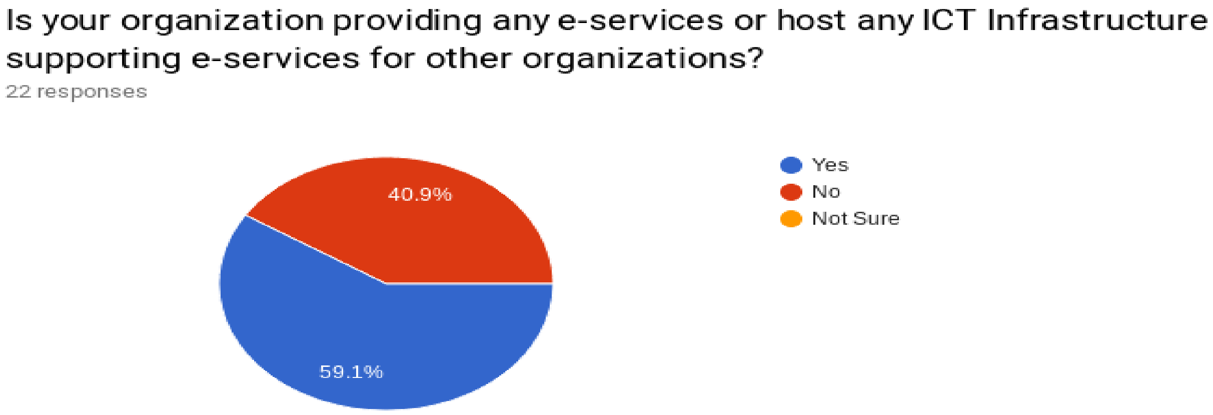
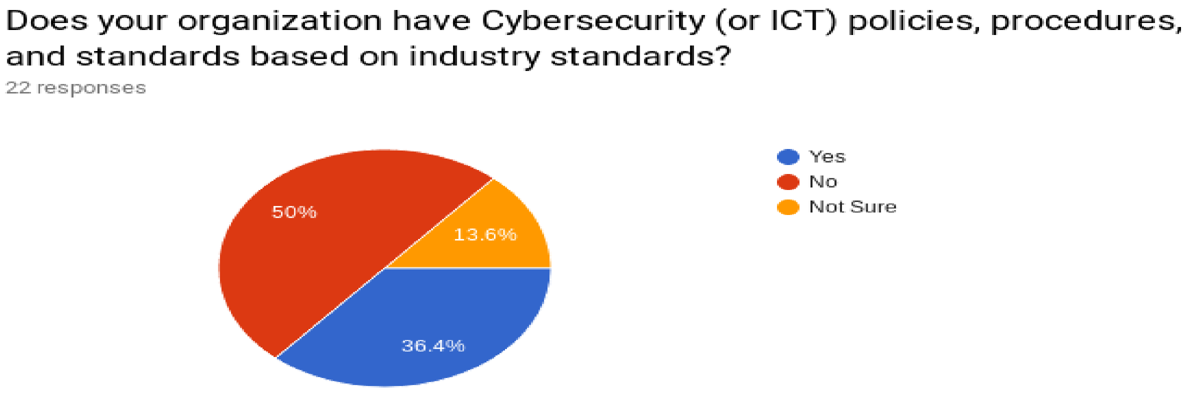


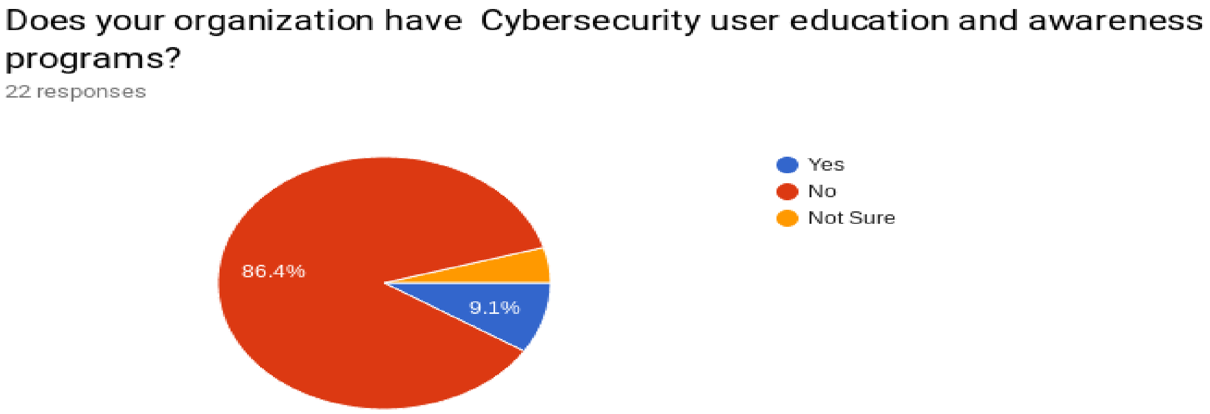
Figure 3. Cybersecurity or ICT Policies



Does your organization have Cybersecurity (or ICT) policies, procedures, and standards based on industry standards?

22 responses

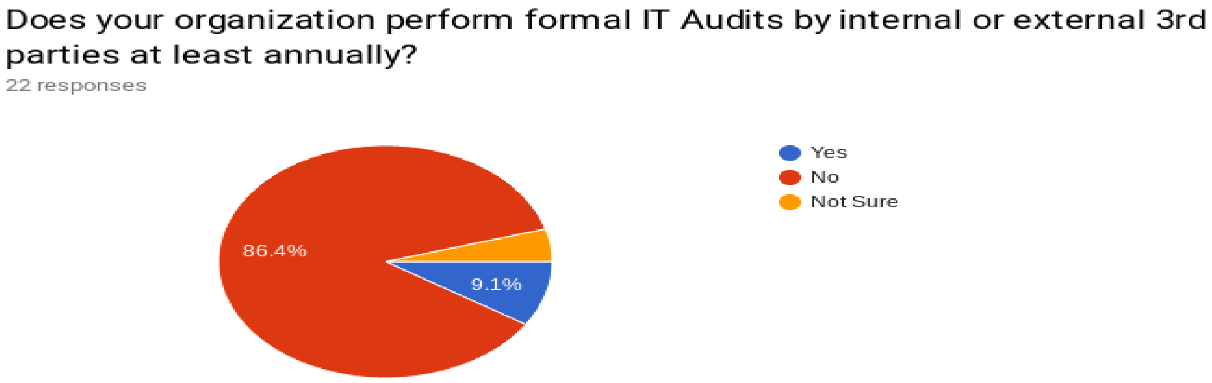
Figure 4. Cybersecurity Awareness and Training



Does your organization have Cybersecurity user education and awareness programs?

22 responses

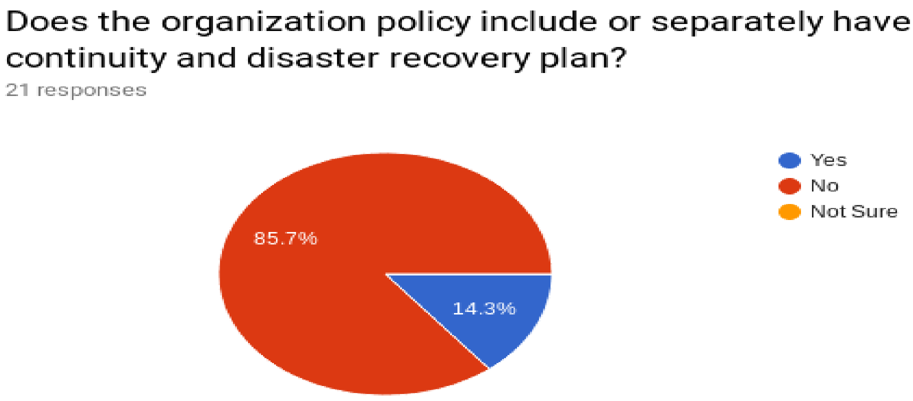
Figure 5. IT Audits/Control Self Assessments



Does your organization perform formal IT Audits by internal or external 3rd parties at least annually?

22 responses

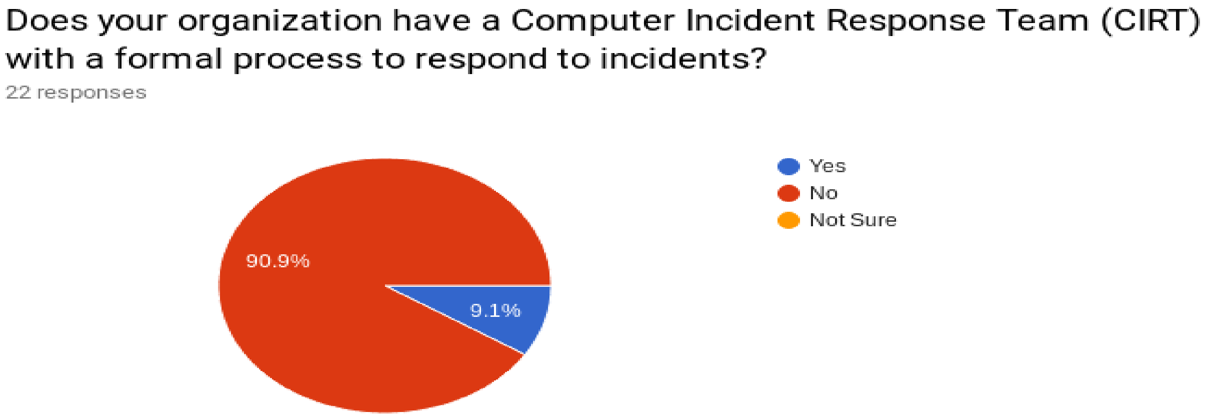
Figure 6. Business Continuity and Disaster Recovery



Does the organization policy include or separately have a business continuity and disaster recovery plan?

21 responses

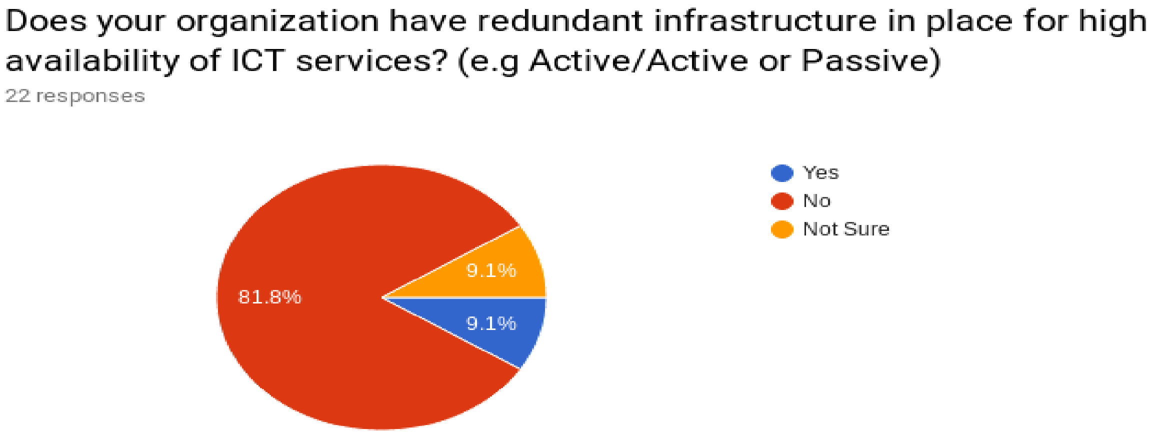
Figure 7. Computer Incident Response Teams



Does your organization have a Computer Incident Response Team (CIRT) with a formal process to respond to incidents?

22 responses

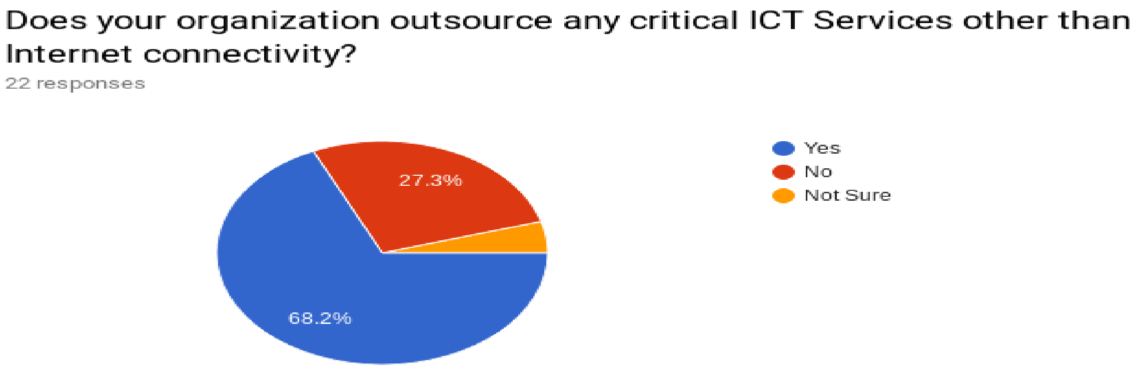
Figure 8. Infrastructure Redundancy



Does your organization have redundant infrastructure in place for high availability of ICT services? (e.g Active/Active or Passive)

22 responses

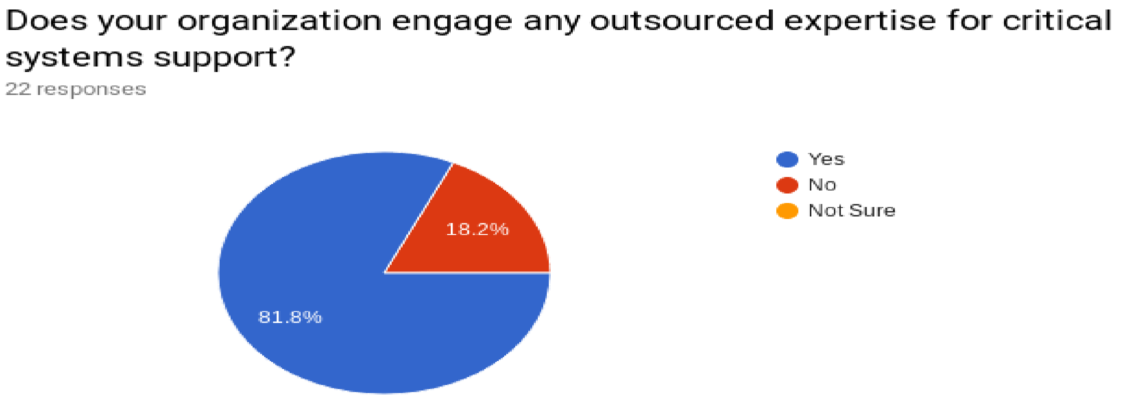
Figure 9. Critical ICT Service Outsourcing



Does your organization outsource any critical ICT Services other than Internet connectivity?

22 responses

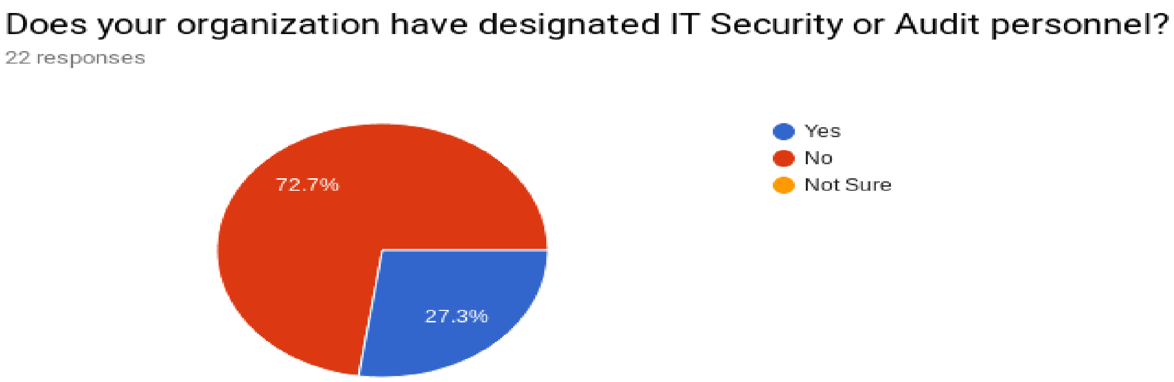
Figure 10. Expertise Outsourcing



Does your organization engage any outsourced expertise for critical systems support?

22 responses

Figure 11. Designated Cybersecurity Personnel



Does your organization have designated IT Security or Audit personnel?

22 responses

Figure 12. Cybersecurity service provision

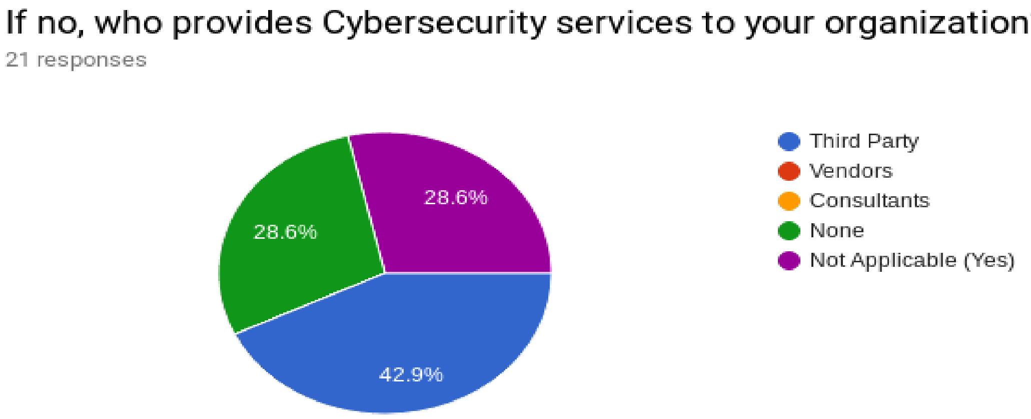
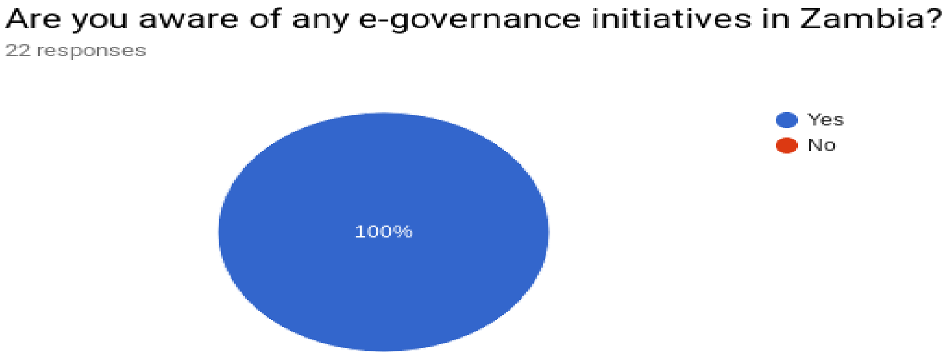


Figure 13. Awareness of e-governance



In summary, the results show slight favorable perceptions towards critical ICT service outsourcing and provision of Cybersecurity by third party. Also about 59% of the organization were providing or supporting e-services.

Respondents who believe Cybersecurity implementation is effective in their organization are less than 50% in all categories. Similarly, the results indicate a more negative perception towards IT Audits, business continuity and disaster recovery planning, redundant infrastructure and awareness and training. Further, the results show that there are respondents ranging from 13% to 20% who neither agree nor disagree with the questions, hence forming a neutral group in some categories. In general, it may be concluded that Cybersecurity implementation regarding the categories in government organization is highly ineffective.

The research findings suggest that Cybersecurity implementation needs further improvement, particularly in areas where respondents' have said no or not sure.

4.2. Discussion and Interpretation of Findings

Firstly, the survey results described earlier are based on the responses provided by the ICT professionals working in different government organizations. Hence, the findings fairly reflect the true state of Cybersecurity situation in the Zambian public sector. The study concludes that Cybersecurity implementation is inadequate to meet the security requirements and objectives of the government organizations.

Secondly, it must be noted from the survey results that there are many respondents (ranging from 13% to 20%) who have neither agreed nor disagreed to the questions with a ‘not sure’ response. Possible reasons for respondents not having any positive or negative feeling towards any Cybersecurity practices may be due to: I) limited/insufficient knowledge of Cybersecurity and ii) little organizational and personal experience of Cybersecurity issues.

Finally, this survey was limited only to government organizations. Including survey participants from the corporate and private organizations may have led to different perspective and thinking.

In this section, the two core issues from the survey objectives above are mapped with the research objective results, to give the final and the most important findings in the research. The first objective was to establish the effectiveness of Cybersecurity practices in Government Institutions in Zambia; Responses indicate that Zambia’s regard to Cybersecurity practices is weak. The second objective was to identify ways of improving Cybersecurity practices in Government Institutions.

Responses and recommendations from respondents as well as from the literature review indicate that capacity building in Cybersecurity would be the first step towards effective Cybersecurity practices. Despite efforts by government towards e-governance initiatives, there is a serious lack of Cybersecurity professionals in Zambia to protect the emerging ICT infrastructure as illustrated in Figure 11. There is therefore an urgent need of investment in Cybersecurity professionals.

From the Cybersecurity categories used in the study, the following are outlined: -

1) **Security and ICT Policy**; ICT Policies, Standards, Procedures and Guidelines are vital for the governance of IT in any organization. It is through such polices that all discussed Cybersecurity practices can be effectively implemented through a top-down approach. From the results of the survey majority of ICT personnel in government institutions are not alive of the existence of the ICT Policy due to either non-existence of the policies or poor communication of policies within the organizations.

2) **IT Audits**; IT Audits are ways in which an organization can verify or test the effectiveness of its Cybersecurity readiness and overall IT governance. IT Audits also test an organization’s compliance

to internal policies as well as external laws and regulations regarding IT. From the survey results, IT Audits are never or poorly implemented in most organizations.

3) **Access Control Management and Secure Infrastructure**; From a technological view, access controls and Secure Infrastructure for the protection of ICTs in organization is insufficient without well trained professions to manage such technologies. From the survey results, there is fairly adequate secure infrastructure of which requires proper management through provision of qualified professionals and guiding policies.

4) **Awareness and Training**; Awareness and training is very necessary in order to provide Cyber aware personnel who understand the importance of Cybersecurity in their organizations. From the survey results, it is evident that such initiatives are poorly implemented in majority organizations.

5) **Business Continuity and Disaster Recovery Planning**; From an operational view, the provision of ICT services at high availability is critical and therefore demands for planning that provides for continuation or quick recovery of such services during and after disruptions to ICT infrastructure. From the survey results, it clear that such practices are poorly implemented.

4.3 Implications

At present moment, any Institution whose operations solely rely on ICTs need to do more to protect themselves from Cyber threats through, IT policies, capacity building and investment in IT security systems.

5. Conclusions and Recommendations

5.1 Conclusion

This paper presents the survey results of Cybersecurity assessment in government Institutions towards e-governance in Zambia. The survey findings show that respondents have favorable responses towards awareness of e-governance initiatives in Zambia. It is also evident that majority of the ICT Personnel were not sure of the existence of ICT Policies due to the fact that they neither existed or were not properly communicated. On the other hand, most respondents had reflected negatively towards awareness and training, business continuity and disaster recovery planning and availability of redundant ICT infrastructure. It was also established that majority organization had no designated IT Security or Audit personnel and the few that exited had no relevant Cybersecurity training or qualifications. There are also respondents who were undecided, which may have changed the survey results had they expressed their opinions. Generally, Cybersecurity practices are inadequate in most developing countries including Zambia and this calls for more policy level effort in order to achieve the level of readiness towards secure e-governance. Without strong Cybersecurity in place, the Zambian government initiatives such as e-governance will not succeed. Cybersecurity will not only be critical to achieving organizational goals and objectives, but also for nation’s economy, security, and critical infrastructure protection.

5.2 Recommendation

This study therefore recommends government institutions in Zambia to establish a Cybersecurity Framework encompassing clear Cyber policy, information systems audit, business continuity and disaster recovery planning, access controls for more secure ICT Infrastructure and Cyber education as well as professional capacity building in Cybersecurity skills in government institutions. Public organizations need to rethink their whole approach to information security and establish security practices needed to protect critical ICT infrastructure. From the Cybersecurity categories in the study, the author recommends the following: -

1) **Security and ICT Policy**; Government Institutions adopted standard ICT policy frameworks that ensure the use ICT facilities and services in an appropriate, secure and risk-appropriate manner, and to ensure that other persons do not misuse those ICT facilities and services. The policies should also undergo annual reviews to keep up with the dynamic environment of ICTs.

2) **IT Audits**; Government Institutions included in ICT policies, mandatory internal or third party IT Audits that are guided by standard frameworks. The Audits to be carried out at least quarterly.

3) **Access Control Management and Secure Infrastructure**; Government Institutions provided intensive Cybersecurity training in order to guide the acquisition, implementation and operational support of secure ICT Infrastructure.

4) **Awareness and Training**; Government intensifies the provision of mandatory awareness and training of all government personnel in Cybersecurity issues.

5) **Business Continuity and Disaster Recovery Planning**; Guided by ICT policies, government institutions included or separately provided detailed business continuity and disaster recovery plans. They also needed to train and grow security experts needed to form computer incident response teams (CIRT) to maintain and secure ICT infrastructure.

Lastly, the author recommends further research on similar and related topics within government institutions.

Acknowledgments

First, I would like to thank the Creator for giving me an opportunity to be one of the first students of the Information and Communication University (ICU) in Zambia. My special gratitude also goes to the entire Zambia Research and Development Centre (ZRDC) team for their partnership with ICU. Further, I would like to thank Dr. Richard Silumbe, my lecturer and supervisor for his guidance and support in previous studies as well as this one.

I would like to extend my gratitude to the reviewers of this paper for their guidance and contributions. I also wish to thank all my students and fellow students for their motivation.

I wish to also say a big thank you to all participants in the survey.

REFERENCES

[1] Bloustein, E. J., 2016. *A Framework for Assessing Cyber Resilience.* [Online]
Available at: https://bloustein.rutgers.edu/wp-content/uploads/2016/05/2016_WEF.pdf
[Accessed 18 May 2018].

[2] Bwalya, K., 2009. *Factors Affecting Adoption of e-Government in Zambia.* [Online]
Available at: citeseerx.ist.psu.edu/viewdoc/download?doi-10.1.1.658.8137&rep=rep1&type=pdf
[Accessed 17 May 2018].

[3] Deloitte, 2014. *Central Asian Information Security Survey Results (2014).* [Online]
Available at: www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf
[Accessed 18 May 2018].

[4] Habeenzu, 2010. *Zambia National ICT Policy.* [Online]
Available at: unpan1.un.org/intradoc/groups/public/documents/unpan/unpan032690.pdf
[Accessed 17 May 2018].

[5] Ipsos, 2017. *Cyber Security Breaches Survey 2017.* [Online]
Available at: https://www.ipsos.com/sites/.../ct/.../cyber-security-breaches-survey-2017-annex.pdf
[Accessed 18 May 2018].

[6] Ipsos, 2018. *Cyber Seurity Breaches Survey 2018.* [Online]
Available at: https://www.ipsos.com/sites/.../ct/.../cyber-security-breaches-survey-2018-annex.pdf
[Accessed 18 May 2018].

[7] ISO, 2017. *International Standards Orginization Security Standards 27001.* [Online]
Available at: http://www.iso27001security.com/html/others.html
[Accessed 18 May 2018].

[8] ITU, 2009. *Readiness Assessment Report for Establishing a National CIRT.* [Online]
Available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/CIRT_Assessment_ABBMN_countries_final.pdf
[Accessed 18 May 2018].

[9] James, C., 2017. *Cyber Security Challenges in Developing Countries.* [Online]
Available at: https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf (2016)
[Accessed 18 May 2018].

[10] Labaree, R., 2009. *The Literature Review - Organizing Your Social Sciences Research.* [Online]
Available at: https://libguides.usc.edu/writingguide/literaturereview
[Accessed 18 May 2018].

[11] Lavrakas, P. J., 2008. *Purposive Sample - Encyclopedia of Survey Research Methods.* s.l., Sage Research Methods.

[12] MOF, 2015. *Lunch of the Center of Excellence of E-Government and ICT by His Excellency.* [Online]
Available at: www.mof.gov.zm/.../245-launch-of-the-center-of-excellence-for-e-government-and-ict
[Accessed 17 May 2018].

[13] MTC, 2017. *Zambia National Data Centre Launch.* [Online]
Available at: https://www.daily-mail.co.zm/data-centre-launch-set/
[Accessed 18 May 2018].

[14] Panos, L., 2011. *ICTs and Development in Zambia: Challenges and Opportunities.* [Online]
Available at: www.panoslondon.panosnetwork.org/wp-content/files/2011/01/panos-london-

zambia-policy-brief-web.pdf
[Accessed 18 May 2018].

[15] Sagepub, 2007. *Ethical Isssues in Conducting Research - Sage Publication.* [Online] Available at: https://www.sagepub.com/sites/default/files/upm-binaries/26094_3.pdf [Accessed 17 May 2018].

[16] Serianu, 2016. *The Africa Cyber Security Report 2016.* [Online] Available at: www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf [Accessed 18 May 2018].

[17] Zhao, H., 2015. *An Investigation on Cyber Security.* [Online] Available at: https://www.researchgate.net/publication/28261309_An_Investigation_On_Cyber Security/ [Accessed 17 May 2018

Appendix

Online Questionnaire Link

https://docs.google.com/forms/d/e/1FAIpQLSfCgvA-fVDFYnRwkl-wJERs6TZqglIvu3F-CoBcE_Qqg584qA/viewform