IST-Africa 2009 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2009
ISBN: 978-1-905824-11-3

e-Government Readiness: An Information Security Perspective from East Africa

Carina K. WANGWE[1], Mariki M. ELOFF[2], Lucas M. VENTER[2]
[1]*University of South Africa, P.O.Box 60049,Dar es Salaam,Tanzania*
Tel: +255 754 600512, Fax: + 255 22 2117772, Email: carina.wangwe@gmail.com
[2]*University of South Africa, P.O.Box 392 UNISA 0003 South Africa*
Tel: +27 12 4296330 Fax: + 27 12 4296771, Email: eloffmm@unisa.ac.za

Abstract: e-Government readiness is the measure by which a government is positioned to provide e-services to its citizens. In order to achieve e-readiness, governments must among other factors, set up efficient collaborations between government agencies. Such collaborations should take into consideration information security requirements. Our study looks at e-government readiness in three East African countries namely, Tanzania, Uganda and Rwanda from an Information Security perspective. Data was gathered through questionnaires and by reviewing country and regional e-government polices, as well as evaluating government agency websites. The results of the study are discussed based on findings by other researches on Information Security and or e-government in the East African region.

Keywords: Information Security, e-Government

1. Introduction

e-Government readiness is the extent to which a government has positioned itself to apply information and communication technologies to provide better access to and delivery of services to citizens, improved interaction with citizens and business, and the empowerment of citizens through access to information. In the East African Community (EAC), which consists of five countries, that is, Uganda, Kenya, Tanzania, Rwanda and Burundi, various initiatives towards delivery of services and citizen participation have been undertaken or are in progress. e-Government Policy documents have been drafted in all these countries except Burundi, and various legislations are being introduced in the arena of e-Government and e-Business[1][6][7][8]. Furthermore an East African e-Government Secretariat has been set up to develop regional policies.

However according to the UN e-Government Survey of 2008 [1], whereas earlier emphasis of e-government was mostly on developing e-services, the focus has shifted towards building and managing integrated and coordinated government services. This is critical since a lack of coordination in policy decisions and announcements can play a considerable role in undermining policy objectives and also weakening the credibility of institutions and policies. Furthermore the report states that ICT-based connected governance efforts are aimed at improved cooperation between government agencies, allowing for an enhanced active and effective consultation and engagement with citizens and a greater involvement with multi stakeholders regionally and internationally. For the case of East Africa, since key infrastructure projects are underway such as the Fibre Optic Backbone projects in Rwanda, Tanzania and Uganda, as well as national ID projects, a good foundation is being laid for government agencies and departments to provide

Copyright © 2009 The authors

integrated services to Citizens. This step however requires the addressing of information security, to ensure confidentiality and integrity of information passed from one agency to another for the purpose of providing a service.

The objective of this study was to evaluate e-Readiness in the EAC from an information security perspective, based on e-government policy documents, cross agency collaborations and government agency websites. Such an evaluation should act as a basis for recommendations as to how government agencies can plan for and address information security in future. The remainder of the papers is structured as follows:

Section 2 gives a brief overview of the information security requirements as indicators of e-readiness. Section 3 explains the methodology used and presents the results obtained. This is followed by a critical analysis of the results with a conclusion and further research in the last section.

2. Information Security e-Readiness Indicators

The security requirements for e-Government can be considered to be:

- Authentication;
- Privacy;
- Authorization and Access Control;
- Data integrity and
- Trust.

The above requirements apply both to transactions between citizens and government agencies and also to inter – agency collaborations. In order to gauge e-readiness from an Information Security perspective, the following factors should be evaluated.

i) The agency should have a information security policy that outlines how and when its systems should be accessed, how trust is established and what standards are there for ensuring privacy and integrity of data. Furthermore there needs to be an enabling environment at country and or regional level in the form of security polices statements incorporated in e-government policies.

ii) The agency should establish standard terminologies for automated transactions to ensure that no misunderstandings arise when dealing with another agency, that is, semantic interoperability is achieved.

iii) The context of the transactions should be taken into consideration and in particular, risks in the inter-agency collaborations should be identified such as the possibility of fraud and network breakdowns.

iv) The incorporation of security requirements in interfaces with citizens, for example, web pages.

Our study therefore investigated whether EAC government agencies or departments have addressed the above factors.

3. Methodology and Results

3.1 Structure of the Study

The methodology used for this study was Grounded theory [2]. The study was conducted between December 2007 and February 2008. Data was collected from three of the five countries forming the EAC, namely, Uganda, Tanzania and Rwanda. Information from Kenya and Burundi was not obtained because of difficulties in communication at the time the data collection was undertaken. Data was collected from three sources i.e.

1. Government Department websites: A review was done of web sites to investigate services offered and any information security related requirements e.g. authentication for e-services.

2. National e-Government policies: A review was done for of e-government and or related documents was done with focus on Information Security.
3. Questionnaires issued to staff of Government Agencies/ Departments. The agencies included in the study were those which as per their operational mandate need to collaborate with other agencies in order to provide a service. The questions designed to address information security requirements identified by several studies including Bakari & Tarimo[3], Chaula et. al[4] both of which were carried out in Tanzania, and from Bakari et.al[5] which is written from a developing countries' perspective. Questionnaires were distributed to Government agencies or departments that typically undertake cross agency transactions.

3.2 Results and Discussion

3.2.1 Web Sites

Twelve websites were examined from government departments/ agencies in the three countries i.e. 4 each. The Criteria for examining web sites was based on the study by Kaaya [6]. The results are represented in Table 1 below:

Table 1: Websites from EA

	Country		
Level (Adopted from Kaaya [5])	Tanzania	Rwanda	Uganda
Initial Level: Web sites are established to provide information about government functions and services	100%	100%	100%
Intermediate Level: Downloadable forms that can be completed and submitted offline are made available on the web site; email interaction between government officials and users may also be supported.	100%	100%	100%
Advanced Level: Web sites begin to support some formal online transactions such as payments or creating and submitting information such as renewing driving license and filing tax returns.	25%	25%	25%
Comprehensive Level: Comprehensive and sophisticated government portals are developed to provide a wide range of information to users coupled with reliable security / privacy/ confidentiality provisions.	0%	0%	0%

The results from the table above show that in all three countries although government agency web sites are available, they have not yet reached the comprehensive level. Thus government agencies need to address how provisions for security, privacy and confidentiality are being made in order to efficiently provide a wide range of e-services to citizens through inter agency collaborations.

3.2.2 Review of Policies

A review of Policy/ Strategy documents related to e-government was undertaken to investigate how information security requirements are addressed. The results were as follows:

i) Rwanda: The Rwanda e-Government Policy Report [7] outlines minimum standards for security both hardware and software and includes also a certification server standard. Furthermore the report states that there shall be a root Certificate Authority (CA) to security certificates to government agencies. The root CA must be trusted by all other CAs. The report does not however state how that trust will be established.

ii) Uganda: The Uganda e-Government Strategy [8], addresses security under the infrastructure component by proposing that a security infrastructure be setup for secure online transactions. A PKI infrastructure is mentioned including a Certificate Authority. Cross Agency collaboration is mentioned as the last phase of the e-government transformation during which agencies will take a whole-of-government perspective when designing and implementing services. Furthermore, the strategy recognises the need to incorporate, within current systems design, the need for among agencies to collaborate in the future.

iii) Tanzania: The National Information and Communication Technologies Policy [9] recognises a need for an e-government infrastructure through which the public service (government departments and agencies) can communicate internally. The policy includes statements that address security in terms of legal framework and infrastructure.

iv) East Africa: The Regional e-Government framework [10] recognises security as a challenge that needs to be addressed in e-government projects. Furthermore, Information Security is recognised as a cross cutting issue and declares that the operational efficiency of any e-government strategy will need strong backup support of necessary legislation on data security, network security, cyber crime, information systems and electronic transactions.

It was found that, all the e-government documents mention information security requirements for inter agency collaborations, although the factors listed in Section 2 of this paper have not been addressed in detail.

3.2.3 Results obtained from Questionnaires

Questionnaires were distributed to government agencies with the objective of soliciting information about information security practices in cross agency transactions. The respondents were managers responsible for technology functions in agencies that engage in cross agency transactions by the nature of their work. Twelve questionnaires were sent out and eight responses were obtained with 4 responses being from Tanzania, and 2 each from Uganda and Rwanda. The questions asked and the responses received are summarised in Table 2 below.

Table 2: Survey Results for Information Security in Cross-Agency Transactions

	Country (No of Respondents)			
Question - Response	**Tanzania (4)**	**Rwanda (2)**	**Uganda (2)**	**Overall(8)**
Presence of Information Security policy - Yes	75%	100%	100%	87.5%
Type of cross agency transactions- Manually	100%	100%	100%	87.5%
Type of cross agency transactions -Email	100%	100%	100%	100%
Type of cross agency transactions -Access to Computer Systems	50%	0%	50%	37.5%
Information involved in transactions - Payment/ Financial	75%	50%	50%	62.5%
Information involved in transactions - Confidential	75%	50%	100%	87.5%
Main concerns in cross agency transactions - Fraud	100%	0%	50%	87.5%
Main concerns in cross agency transactions - Network Breakdowns	50%	0%	100%	50%
Security measures such as encryption - Yes	75%	100%	100%	87.5%
Binding agreements with regards to information security with partners - Yes	50%	0%	0	50%
Common format for Data Exchange - Yes	50%	0%	50%	37.5%

	Country (No of Respondents)			
Question - Response	**Tanzania (4)**	**Rwanda (2)**	**Uganda (2)**	**Overall(8)**
Common terminology for transactions - Yes	0%	0%	50%	12.5%
Need for standards for cross agency transactions - Yes	100%	100%	100%	100%

3.2.4 Discussion

From the above results the following observations are made:

- There is no significant difference in results between the three countries.
- There appears to be a correlation between the presence of an information security policy and the use of security for transactions. The agency without a security policy has no security measures in place for transactions.
- Fraud is a major concern in over 50% of the respondents
- Fraud is a bigger concern than network breakdowns.
- A need for standards is recognized by all agencies although only 37.5% and 12.5%of the respondents have common terminology for transactions and common data format exchange respectively.
- Although in the case of Rwanda the e-government report mentions that requirements/ standards of security, the questionnaires returned do not refer to the document, thus posing the question of whether government agency are aware of the standard.

4. Conclusions and Further Work

The results of our study show that from an Information Security perspective, some steps have been taken towards improving e-readiness in the East African community at an agency, country and regional level. However the of the factors outlined in section 2 of this paper are yet to be fully addressed. It can be concluded that the EAC has not fully reached e-readiness. The results of this study can also be related to work done by Rwangoga & Baryayetunga [11] who discuss e-Government in Uganda and describe successful delivery on institutional frameworks, legal frameworks, and ICT infrastructure.

In order to enhance e-readiness for an Information Security perspective, the following recommendations are made for East African countries:

i) The establishment of government – wide guidelines that encourage the establishment of Information Security policies in all government departments and agencies. The policies should address both inter and intra agency transactions as well as security requirements for interfaces with citizens.

ii) The establishment of Risk Management Frameworks for e-government transactions. The risk frameworks should identify risks and how to mitigate those risks.

iii) The establishment of an e-government security ontology for East Africa to ensure semantic interoperability. This could be modelled on the e-government ontologies that have been developed in the European Union [12] and United States[13].

In future research, we plan to look further at the development of a holistic framework to address Information Security in e-government. Such a framework would address standards, common terms, infrastructure and policies, all from the context of developing countries, and in particular, East Africa.

References

[1] UN E-Government Survey 2008: From E-Government to Connected Governance. 2008.

[2] R. M. De Villiers, Three Approaches as pillars for interpretive Information Systems Research: development research, action research and grounded theory. In proceedings of SAICSIT, 2005.

ACM.2005

[3] J.K. Bakari, C.N. Tarimo, L.Yngstrom, and C. Magnusson, State of ICT Security Management in the Institutions of Higher Learning in Developing Countries: Tanzania Case Study, In Proceedings of the Fifth IEEE International Conference on Advanced Learning Techniques (ICALT'05). IEEE. 2005, pp 1007-1011.

[4] J.A. Chaula, L. Yngstrom, and S. Kowalski, Technology as a tool for Fighting Poverty: How Culture in the developing world affect the Security of Information Systems. In proceedings of the 4th IEEE International Workshop on Technology for Education in Developing Countries. IEEE. 2006, pp 66-70.

[5] J.K. Bakari, C.N. Tarimo, and B. Mutagahywa, Issues and Challenges to be Addressed in e-Government from an Information Security Point of View, In Proceedings of IST-Africa 2006 Conference, IIMC, 2006.

[6] J. Kaaya, The Emergence of E-Government Services in East Africa: Tracking Adoption Patterns and Associated Factors. In proceeding of Sixth International Conference on Electronic Commerce. ACM. 2004, pp 438-445.

[7] Rwanda Information Technology Authority: Technical Standards and Guidelines for E-Government: Final Report, February 2006

[8] Republic of Uganda, Ministry of Works, Housing and Communications, E-Government Strategy and Action Plan Ver 1.1, Mar - 2004

[9] The United Republic of Tanzania, Ministry of Communications and Transport, National Information and Communications Technologies Policy, March 2003

[10] East African Community Secretariat, Regional e-Government Framework (Final Draft), December 2005

[11] N.T. Rwangoga, and A.P Baryayetunga. E-Government for Uganda: Challenges and Opportunities. International Journal of Computing and ICT Research, Vol.1 No. 1 June 2007, pp 36-46.
European Union, Access e-Gov Project,

[12] http://www.accessegov.org/acegov/web/uk/index.jsp?id=50024, accessed 4 Feb 2009.
Federal Enterprise Architecture Reference Model Ontology, http://web-services.gov/fea-rmo.html, accessed 4 Feb 2009