Information Security challenges and their implications for emerging e-government structures in some African Countries

Kyobe M.E.
University of Cape Town

Abstract

Governments in the developing world have invested substantial resources in e-government to increase convenience in service delivery, education, information sharing and transparency in their activities. However, while these initiatives provide much promise in addressing the needs of citizens, poor security measures threaten their success. Limited research has been conducted to address information security challenges in e-government. The present study examines information security issues and their implications for the emerging e-government structures in Africa. Literature on governance and e-government was reviewed and the findings show that the causes of insecurity have been limited to technological and economic factors. The researcher shows however that politics, culture, regulations and moral behaviors pose serious threats to e-government security today. A more holistic approach to the analysis and design of information security is therefore recommended in this paper.

Introduction

Governments in the developing world are investing substantial resources in e-government with a view to increase convenience in service delivery, education, information sharing and transparency in their activities (Kaisara and Pather, 2009). However, while these developments provide much promise in addressing the needs of citizens, the lack of security, confidentiality and access to accurate information present major challenges for e-Government initiatives (SITA, 2002; Farelo and Morris,2006; Kaisara and Pather, 2009).

Little is still known about information security challenges involved in e-government. Most studies on e-government seem to focus mainly on planning and developmental processes (Farelo & Morris, 2006:11;Kaisara and Pather, 2009). The draft paper on information security (Dept of Public service and administration, n.d. p2) emphasises that: “e-government security will assist profoundly in the bridging of the chasm of the digital and knowledge divide that exist within our country, as well as encourage the average citizen to participate more in the public domain thereby bringing the benefits of democracy to the people”.

Karokola and Yngström (2009) also observed that while there are several maturity models to guide and benchmark e-government developments in developing countries, (e.g., Layne and Lee’s four stage model; Chandler and Emanuel’s four stage model; Gartner’s four stage model; United Nation’s five stage model; West’s

four stage model, and others), limited consideration is given to technical and non technical security issues.

The present study examines information security issues and their implications for the emerging e-government structures in Africa. The author begins by discussing the concepts of governance and e-government. The role ICT plays in ensuring governance is examined followed by a review of some theoretical work explaining the causes of poor information security. Examples of security challenges drawn from e-government initiatives in some African countries are then presented. Finally conclusions are drawn and recommendations are made.

.

E-government and Governance

While the terms government and governance share the same root words, governance has more to do with government. Government is the institution or those in authority given the responsibility of ensuring governance. Governance relates to the broader relationships between citizens and institutions. Governance may be defined as a mechanism to provide accountability for the way an organisation manages itself or a set of rules that frame behaviour (OECD, 2002, 2004). Institutional economists define governance as rules linking together actors, individuals and organisations, Finger (2005). E-governance on the other hand seeks to support processes and structures for harnessing the potentialities of ICTs to empower citizens through better democratic processes, service delivery and good governance (Misuraca, 2006; SITA, 2002).

Bélanger and Hiller (2005:20) provide a broader description of the domains of e-government: government with individuals in relation to delivery of services (e.g., where the government establishes or maintains a direct relationship with citizens to deliver a service or benefit); government with individuals in relation to political process (e.g., the relationship between the government and its citizens as part of the democratic process like voting online); government with business as a citizen whereby opportunities for business with the government are created, (e.g., by providing securities exchange commission, filings online or paying taxes online); government with business in the marketplace (e.g., transactions involving procurement or hiring of contractors or acquisition of goods and services by the government); government with employees (which involves online relationships between government agencies and their employees, e.g., using an intranet); and government with government (where government agencies collaborate and/or provide services to one another).

Governance and ICT

Much of the literature on e-government has focused on the contribution of ICT in mitigating governance problems. However, according to Finger (2005), the impact of

ICT on governance is not only positive. ICT can also exacerbate governance problems. This influence of ICT on governance can be explained by the Institutional theory (New institutionalism) and ICT adoption theories.

Institutional theory & New institutionalism

Institutional theory considers how structures such as values, norms, rules and procedures become established as authoritative guideline for social behaviour. It inquires into how these elements are created, diffused, adopted, and adapted over space and time; and how they fall into decline and disuse (Scott 2004a). Scott adds that "Although the ostensible subject is stability and order in social life, students of institutions must perforce attend not just to consensus and conformity but to conflict and change in social structures" (Scott, 2004a).

Related to this is the theory of New institutionalism (March and Olsen, 1984) which holds that behaviour is fundamentally moulded by the institutions it is embedded in. New Institutionalism recognizes the fact that institutions do not operate in a vacuum, but in an environment (institutional environment), consisting of other institutions. They pressurise each other and impact on human behaviour, and in these transformational processes, new governance structures and challenges arise.

Governance challenges arising from Institutional (State) transformation

One major factor driving transformation in States is globalisation. This has caused various changes in the way States operate. First, there is an emergence of non-state actors like transnational corporations (TNCs) and non-governmental organizations (NGOs), with which the State has to share power (Finger, 2005). Mengisteab (2008) also observed that globalisation has facilitated the reconstruction of the States in Africa by shifting the balance of power between State and Society in favour of society. Second, public affairs are increasingly managed at levels other than the nation-state level (e.g., the emergence of supra-national levels - EU, global and regional bodies), Finger (2005). Third, there is growing separation of the State functions of service delivery, rule-making and regulatory tasks (Finger, 2005). Mengisteab (2008) also observed that globalisation and its liberalization policies have narrowed the discrepancy between policy and social interest. He asserts that policy-making in Africa is increasingly controlled by external institutions such as the IMF and donor countries.

According to Finger (2005), public affairs are becoming more fragmented (functions), diluted (levels) and outsourced (to non-state actors). This means therefore that for these services to be rendered effectively and legitimately, the State has to collaborate with these non-state actors. This requires new and complex governance structures which usually take the form of partnerships between public and private operators and other mechanisms of public intervention into the market (Finger, 2005).

The influence of ICT on Governance

ICT is part and parcel of this evolution. It sustains the evolution and also reacts to it. Finger (2005: 1-7) argues that ICTs actively push this evolution further, thereby leading to the involvement of more non-State actors in public affairs. On the other hand, ICTs are also developing in reaction to the challenges posed by this very evolution by offering solutions to link the different types of actors and new ways of performing the various State functions. Finger cautions however that while ICT can mitigate governance problems, it can exacerbate them at the same time.

For example, when the State and non-state actors engage in a contractual arrangement, information asymmetries may arise. These asymmetries can be reduced by introducing ICT and ensuring that both parties have access to the technologies. However, if such access is not distributed equally, the same technologies will worsen information asymmetries, thereby exacerbating governance challenges significantly (Finger, 2005). One typical area where ICT has created serious challenges for e-government today is in information security. This is examined in more detail in the following sections of this paper.

Information security challenges in e-government

While information security has become a major issue for many institutions and initiatives today, there have been limited studies examining security problems in e-government (Karokola et al.,2009). Existing literature also tends to focus more on technology and economic issues (Westerlind, 2004; Theodosios and Stephanides, 2005). However, there are many other non-technology factors contributing to insecurity in institutions. These include cultural, social, legal, moral and political factors. The researcher argues that a more holistic approach to security needs to be adopted if effective solutions to information security challenges are to be found. In the following sections, the above factors are discussed in more detail and some examples showing how these have influenced e-government projects in some African countries are presented.

Culture and social issues

Many studies have linked the problems of information security to employee bahaviors and the culture of the organisation. Citing the work of several writers on culture (e.g., Thomson, von Solms, & Louw, 2006; Siponen & Oinas-Kukkonen, 2007; Dhillon, 1997), Lim, Chang, Maynard and Ahmad (2009: 88-91) distinguish between Organisational Culture (OC) and Information Systems Culture (ISC). They state that OC refers to “systems of shared beliefs and values that develops within an organization and guides the behaviours of its members to maintain suitable patterns of social systems to form a coordinated behaviour to survive in the dynamic environment” while ISC is “the totality of patterns of behaviour in an organization that contribute to the protection of information of all kinds”. They concur with Dhillon (1997) who maintains that OC is necessary to maintain the integrity of the organizations and also to protect the technical systems of the organizations. They maintain that this can be achieved by instilling the aspects of information security in every employee’s daily tasks. Lim et al (2009) however caution that the task of embedding information security culture into the organisational culture is complicated

by factors such insufficient security budgets; locus of responsibility, organizational motivation towards implementing security measures, and the different perceptions towards security risk.

Technological issues

The adoption of technology brings with it various issues relating to the infrastructure, communication, access rights and abuse of privacy, data protection, digital signatures, firewalls and viruses. For instance, when existing IT infrastructure is not fully integrated into the business processes and optimized to perform efficiently and effectively, this may impact on the control, quality and speed of information access, and the availability of information. Communication can be impeded or made vulnerable to attacks by the quality of infrastructure in place (e.g., bandwidth; type of hardware and software used). Social-media can enable learning and sharing of knowledge but often leads to abuse of privacy and data.

Legal issues

While a number of regulations have been implemented to ensure security and privacy of information, citizens and organisations sometimes find them restrictive and demanding compliance with several requirements. In the US, for instance the government restrict the use of cookies on their sites (Belanger and Hiller, 2006). Regulations like the protection of personal information require that agents comply with numerous provisions. For instance, agencies that maintain records about an individual must give notice of new records, make them accessible, ensure accuracy, allow individual inspection, obtain permission to share the information and inform the individual of the uses for the information (Belanger et al., 2006).

The regulations have also been found to lack in their enforcement mechanisms and penalties (Furlong, 1991). In Australia, citizens were concerned about the lack of severity of penalties invoked on spammers (Vircom.com, 2004) and in South Africa, Internet users have to live with Spam since it is not illegal per se. Similar sentiments have been expressed in the United States over the CAN-SPAM Act of 2003. Critics argue that this Act may potentially increase the amount of spam by providing a set of guidelines for spammers on how to spam legally (Zhang, 2005). In South Africa, SBP (2005) argues that many regulations are made on the incorrect assumptions that all citizens (including those in rural areas) are equally literate and understand English or Afrikaans. This limits the awareness and understanding of the law.

Moral and Ethical issues

Ethics has been described as code of conduct considered by society as right and good and is usually based on the notion of morality, values and faith (Land, Amjad, and Nolas, 2007). Un-ethical practices undermine the generation, transmission and sharing of information. According to Floridi (2006), evil and immoral behaviors are attributed to deficiency of information. He identifies three ways by which the integrity

of a moral person may be compromised during information processing. First, when information is used as a resource, moral issues such as availability, accessibility, accuracy of information sources, reliability and trustworthiness of information sources arise. Second, when information is used as a product, moral issues relating to accountability, liability, plagiarism, propaganda and misinformation may arise. Third, when the actions of the agent affect the information environment (i.e., information used as a target). Moral issues that arise include breach of someone's information privacy and confidentiality, unauthorised access to systems and other security issues. Sometime the cross-referencing (aggregation) of data also creates privacy risks. This may happen when government departments merge or share information. Agencies share information with other agencies for various purposes, such as debt collection, identification and eligibility verification. This is often done without the consent of the information owner.

Political issues

Politics has a great impact on security. Corrales and Westhooff (2006) state that factors typically associated with high growth rates, such as labor productivity, financial mobilisation and export competitiveness require some degree of domestic technology sophistication. They maintain that technology adoption is connected to issues of political liberties: "On one hand, knowledge-based technologies may foster liberties, democratization, human rights and societal empowerment. On the other hand, the propensity to adopt new technologies in turn depends on existing liberties". They observed that states that repress political and economic rights are less likely to adopt liberty-promoting new technologies. However, they also found that not all authoritarian regimes discourage internet use similarly: "High-income, market-oriented autocratic states are less draconian. Although they fear the political consequences of internet expansion, they also welcome its economic payoffs".

E-government security challenges – examples from Africa

In this section, the author highlights some of the security challenges facing e-government in Africa resulting from technological, social, cultural, legal and political influences

Technology related issues:

Kaisara and Panther (2009) identified trust in systems as a major impediment to e-government initiatives. In a study that examined usage of internet at provincial and local level in South Africa, Meyer (2007) found that most users were unhappy with the use of the internet to seek services. Frustration and lack of interest in the systems could result in lack of attention to security, data capturing errors and potential abuse of systems. Ngulube (2007) also found that many government websites are not fully functional and they are populated with information that does not enhance service delivery and participatory democracy. In addition they also affect the confidence of buyers and organisations intending to do business with the

government. Onyancha (2007) analysed the up-to-datedness of government websites in East and Southern Africa and found that majority did not provide copyright dates and when the websites were updated. Copyright is intended to protect intellectual property against abuse, theft and other violations of the rights granted by those statutes to the IP owner. If this is not indicated or updated on the website, this could lead to copyright infringement.

Karamagioli, Koulolias and Berntzen's (2008) study of African parliaments reveal that many African countries possess insufficient ICT infrastructure and lack reliable and adequate access to the internet. This limits parliamentarians' ability to access information necessary for decision making. Use of unreliable infrastructure exposes the system to hacking, virus attacks and other security risks.

Heeks (2002) reports that in many African countries, data quality and data security are very poor and there are few mechanisms to address these issues. He states further that digital signatures cannot be accepted in some countries. He concludes that while there have been some progress in e-government, much has to be accomplished in terms of computing and telecommunications infrastructure in Africa. These sentiments are also shared by Gichoya (2009) in Kenya.

Legal Issues:

Citing the work of several writers, Magele (2006) presents several concerns over the current security regulations in South Africa. In particular, the ECT Act does not say much of the standards of electronic filing or processing and leaves gaps for criteria for authentication of signatures. There were also concerns that this Act might seek to grant the state discretion as to whom it may register and that it could limit technologies that could be deployed in encrypting data messages. The provision in the Consumer protection chapter that customers can return goods within 14 days if unhappy and also have a seven day cool off period to cancel a transaction without reason or penalty and obtain a refund excludes, e.g., the financial services sector, auctions and daily consumables.

Magele (2006:8) also raises the problem of databases and cross referencing. He argues that there are many unknown databases with citizen personal profiles, not known to the citizens and the database custodians continue to retain such information without people's consent. He argues that the law fails to state how it will restrict sharing of such information or regulate existence of illegal private information solicitation.

Moral and Ethical issues

On e-crime in South Africa, Magele (2006) claims that most activity is in the financial services industry and it involves mainly stealing identify for financial transactions, immigration, marriage certificates and citizenship. A report by the African Information security association (2009) highlights several online dangers to students using the internet in Africa. These include adult pornography, internet fraud, online violence,

hate culture, gambling, sexual solicitation, impersonation, etc (breach of privacy and confidentiality). There are also reports on increasing cyber attacks on government websites in South Africa (PublicTechnology.net,2008; Engelbrecht, 2008).

Cultural issues

Udo (2007) found that citizens did not have much interest in municipal information systems. When asked about their satisfaction with the methods through which they receive information, 54% preferred receiving information through South African post office, 34% via email and only 9% preferred the internet. When respondents were asked whether their business organisations would be interested in interacting with eThekwini municipality using the Internet as a communication medium, 41% percentage responded negatively. This could have much to do with the established trust and confidence in the postal services to deliver documents safely as compared with the risky Internet. Udo suggested that there is a need for appropriate ICT infrastructures and effective interaction mechanisms that would build confidence and enable better use of ICT for service delivery.

There is also evidence to suggest that a culture of information security has not been developed in e-government. Bakari,Tarimo and Mutagahywa (2006) report that information security has not received the required attention in Tanzania. Ngobeni and Globler (2009) examined information security policies of some governmental organisations in South Africa. They found that policies were not comprehensive enough – e.g. missing data classification and control; risk assessment; security awareness and training; data privacy management; communication security; document destruction and retention. Their study showed that most of these governmental organisations omit the most significant issues that are relevant to ensuring effective information security.

In his analysis of the findings of the study on global e-government status by the centre for public policy - Brown University, Mutula (2008) report that sub-saharan Africa member states fared badly among 198 countries ranked. The e-government status study assessed government web sites for the presence of features dealing with information availability; digital signatures, online database, credit card payment, etc. None of the African countries was among the top perfomers. In their paper on rethinking e-government development – Cape Gateway Portal, De Tolly, Maumbe and Alexander (2006) identified lack of monitoring and evaluation as major limitations. They state that although log file statistics are analysed regularly, these usually fail to indicate who is using the portal and how and there were many user interface problems. Lack of transparency and accountability increase the level of fraud and corruption. Further, they state that most government departments have limited capacity and skills in content creation and web publishing. They argue that

user analysis would be crucial to the identification of user needs. It may also be suggested that such evaluation would reveal potential security risks in the system.

De Tolly, Maumbe and Alexander (2006) also found that there was a clash of organisational cultures whereby Portal staff were often seen as outsiders, i.e., not government staff. This resulted in lack of trust.

Political

A good example on how politics may influence ICT adoption is Zimbabwe. According to the World Economic Forum's *Global Information Technology Report, Zimbabwe was ranked* 105th out of 115 economies in 2005-2006, based on a networked readiness index, which measures the degree of preparation of a nation to participate in and benefit from ICT developments. Many of the problems can be trace back to the political situation in the country. Mutula (2008) confirms that limited progress in e-government has been made in Zimbabwe and that the countries web portal contains minimal information for the common citizen. Kaitano (2010) alleges that most senior executives and board members in Zimbabwe give a blind eye to Information security governance.

A study conducted earlier by Barata, Cain and Serumaga (2000) found several weaknesses in the records management and accounting system in Zimbabwe. They found that accounting clerks do not receive training in how to manage records properly and there were no effective tracking mechanisms. They state further that where problems occur, there is no recognised authority that can enforce compliance with records legislation or pursue disciplinary action. This significantly undermines the Government's effort to implement computerised financial management systems.

Conclusion

The objective of this study was to examine information security issues in emerging e-government structures in Africa. This area has been neglected in e-government research, yet it is critical to the success of e-government initiatives. A review of existing literature shows that ICT can mitigate and also exacerbate governance problems. This study focused on the latter and the review of literature confirms that information security is a major limitation caused not only by technological developments as normally perceived in literature, but also by political, cultural, legal and moral behaviors of the society. Further, while the security challenges faced in e-government may not differ from those in the private sector, they are more complex and sensitive because e-government operations involve many citizens and are bound to various legal frameworks and requirements. Investigating such complex problems requires a holistic approach. Existing approaches used in the analysis of e-government security problems are not comprehensive. The findings presented in the present paper are based on evidence gathered in a few countries therefore

precautions need to be taken in generalizing these findings. It is recommended however that empirical research, based on holistic approaches, be conducted in future to examine and measure the individual, combined and potential moderating effects of technological, economic, social, cultural, legal and political factors on e-government security in Africa countries.

References

African Information Security Association (2009). Report of children & young people online protection forum to mark the world telecommunication and information society day. Lagos, Nigeria. Retrieved February 20, 2010 from: http://www.jidaw.com/security/aisa/protecting_children_online_aisa_report.html

Bakari, J., Tarimo, C. and Mutagahywa B. (2006). Issues and Challenges to be Addressed in e-Government from an Information Security Point of View. IST-Africa 2006 Conference Proceedings Paul Cunningham and Miriam Cunningham (Eds) IIMC International Information Management Corporation, 2006

Barata, Cain and Serumaga (2000). From Accounting to Accountability: Managing Accounting Records as a Strategic Resource. Zimbabwe: A case Study. Report to World Bank infoDEV Programme. International Records Management Trust (2000). http://www.irmt.org/documents/research_reports/accounting_recs/IRMT_acc_rec_zimbabwe.PDF

Bélanger, F. & Hiller, J. (2005) A framework for e-government: Privacy implications. *Business Process Management Journal*, **11**,

Corrales J., and Westhoff, F. (2006). Information Technology Adoption and Political Regimes. International studies quarterly, 50: 911-933.

Dept of Public service and administration (n.d) http://www.dpsa.gov.za/documents/acts&regulations/frameworks/e-commerce/POSITION%20PAPER%20ON%20INFORMATION%20SECURITY1.pdf

Engelbrecht, L. (2008). Fraud flies in Q1 2008. ITWeb 18 April 2008. Retrieved April 20, 2008 from www.itweb.co.za/sections/business/2008/0804181100.asp

Farelo, M and Morris, C. (2006). The Status of E-government in South Africa. IST Africa Conference, Pretoria, South Africa, 7-9 May 2006, pp 1-12. Retrieved April 14, 2010, from: researchspace.csir.co.za/dspace/bitstream/10204/966/1/Farelo_2006_D.pdf

Finger, M. (2005). Conceptualizing e-Governance. Retrieved April 20, 2010, from: www.politech-institute.org/review/articles/Finger_Matthias_volume_1.pdf

Floridi, L. (2006). " Information Technologies and the Tragedy of the Good Will", Ethics and Information Technology, Kluwer Academic Publishers, Netherlands, 2006, 8(4): pp. 253-262.

Furlong, W.J. (1991). The Deterrent Effect of Regulatory Enforcement in the Fishery. *Land Economics,* 67(1), 116-29.

Gichoya, D. (2009). Facing the challenges of ICT implementation in Government. IST-Africa 2009 conference proceedings, Paul Cunningham and Miriam Cunningham (Eds). IIMC, 2009

Heeks R. (2002). eGovernment in Africa: *Promise and Practice, Paper 13,* Institute for Development Policy and Management. http://idpm.man.ac.uk/wp/igov/index.htm

Kaitano, F. (2010). Information Security Governance: Missing Link In Corporate Governance. http://www.techzim.co.zw/2010/05/information-security-governance-missing-link-in-corporate-governance/

Kaisara, G., and Pather, S. (2009). E-Government in South Africa: e-service quality access and adoption factors. Proceedings of the 11th Annual Conference on World Wide Web Applications. Port Elizabeth, 2-4 September, 2009.

Karamagioli, E., Koulolias, V., and Berntzen, L. (2008). Challenges and Barriers of Introducing ICT to Enhance Functioning of Parliaments.
IST-Africa 2008 Conference Proceedings Paul Cunningham and Miriam Cunningham (Eds) IIMC International Information Management Corporation, 2008

Karokola, G. and Yngström, L. (2009). Discussing E-Government Maturity Models for Developing World Security View. Proceedings of the ISSA 2009 Conference, 6-8 July, 2009, University of Johannesburg.
http://icsa.cs.up.ac.za/issa/2009/Proceedings/ISSA2009Proceedings.pdf

Land, F., Amjad, U., and Nolas., S. (2007) "The Ethics of Knowledge Management". IJKM, IGI Global, 2007, 3(1) pp.1-9.

Misuraca, G. (2006), e-Governance in Africa, from theory to action: a practical-oriented research and case studies on ICTs for local governance. Retrieved Mar 15, 2010, from
http://delivery.acm.org/10.1145/1150000/1146659/p209-misuraca.pdf?key1=1146659&key2=7885861821&coll=GUIDE&dl=GUIDE&CFID=97993104&CFTOKEN=65629072

Magele T. (2005). E-security in South Africa. White paper, ForgeAhead e-security event, 16-17 February, 2006

March, J.G., and Olsen, J.P. (1984). “The New Institutionalism: Organizational Factors in Political Life.” American Political Science Review 78 (September): 734–49

Mengisteab, K. 2008. Globalization in Africa-Globalization’s implications for Africa. Retrieved June 10, 2010, from http://216.239.59.104/search?q=cache:pjToVdQfifQJ:science.jrank.org/pages/9529/G1...

Meyer, J.A. (2007), “E-governance in South Africa: making the populace aware – an Eastern Cape perspective, communities and action”, paper presented at CIRN Conference, Prato, Italy, November, .

Mutula, M. (2008). Comparison of sub-Saharan Africa's e-government status with developed and transitional nations. Information Management & Computer Security, 16(3), 2008.

Ngulube, P. (2007). The Nature and Accessibility of E-Government in Sub Saharan Africa
International Review of Information Ethics 7(9) 2007. Retrieved January 20, 2010 from http://www.i-r-i-e.net/16-31.htm

Ngobeni,S.J, and Globler, M. (2009). Information security policies for governmental organisations, The minimum criteria. ISSA 2009.

OECD (2002). Highlights - OECD Information Technology Outlook 2002. Retrieved January 10, 2009, from www.**oecd**.org/data**oecd**/63/60/1933354.pdf

Onyancha, M. (2007). E-governance in Eastern and Southern Africa: a Webometric study of the Governments’ websites - Up-to-datedness of government websites. International Review of Information Ethics 7(9) 2007. Retrieved 20 June, 2010, from http://www.i-r-i-e.net/16-31.htm

PublicTechnology.net (2008). Cybercrime syndicate scoops millions from South African government. Retrieved June 13, 2008, from http://www.publictechnology.net/modules.php?op=modload&name=News&file=article&side=16110.

SBP - Strategic business partnership for growth in Africa (2005). The impact of sector-specific policies and regulations on the growth of SMEs in 8 sectors of the SA economy . Retrieved February 10, 2007, http://www.thepresidency.gov.za/docs/pcsa/economic/sbp.pdf

Scott, R. (2004). Institutional Theory: Contributing to a Theoretical Research Program. Chapter prepared for *Great Minds in Management: The Process of Theory Development,* Ken G. Smith and Michael A. Hitt, eds. Oxford UK: Oxford University Press. http://icos.groups.si.umich.edu/Institutional%20Theory%20Oxford04.pdf

Scott, W. Richard 2004b. "Institutional theory." Pp. 408-14 in *Encyclopedia of Social Theory,* George Ritzer, ed. Thousand Oaks, CA: Sage
Lim JS, Chang S, Maynard S & Ahmad A. (2009), Exploring the Relationship between Organizational Culture and Information Security Culture. 7th Australian Information Security Management Conference. 88-97. Churchlands, Australia: Edith Cowan University.

SITA (2002). e-Government experience in South Africa. SITA. Retrieved January 10, 2009, from: unpan1.un.org/intradoc/groups/public/.../UNPAN006470.pdf

Theodosios., T., and Stephanides G. (2005). The Economic Approach of Information Security. Computers & Security. No.24. 105-108.

Udo, A. (2007). A Framework for a Municipal Information Society in South Africa. *IST-Africa 2007* Conference Proceedings Paul Cunningham and Miriam Cunningham (Eds) IIMC International Information Management Corporation, 2007

Vircom.com (2004). Can Laws Block Spam? An analysis of the effect of international spam legislation. White paper, Vircom, 2004.

Westerlind K (2004). Evaluating. Return on Information Technology Investment. School of Economics and Commercial Law. Gothenburg University.

Wimmer M, Von Bredow B. 2002. A Holistic Approach for Providing Security Solutions in EGovernment. System Sciences. HICSS. Proceedings of the 35th Annual Hawaii International Conference. Hawaii: 7-10. 1715-1724.

Zhang, L. (2005). The CAN-SPAM Act: An insufficient response to the growing Spam problem. Berkeley Technology Law Journal, 20, 301-332.