SECURITY, PRIVACY & TRUST ISSUES SURROUNDING E-COMMERCE IN KENYA

[1]MWENCHA, PETER MISIANI, [2]MUATHE, STEPHEN MAKAU, [3]THUO, JOHN KURIA,

[1] PhD Candidate, Department of Business Administration, Kenyatta University, Nairobi, Kenya

[2] Lecturer, Department of Business Administration, Kenyatta University, Nairobi, Kenya

[3]Assoc. Prof., School of Business, Gretsa University, Thika, Kenya

E-mail: mwencha@hotmail.com, muathesm@yahoo.com, thuokuria@yahoo.com

Abstract

The growth in internet usage in Kenya has been characterized by a proliferation of various online-based electronic commerce services. However, much as this growth in usage has created various business opportunites, it has also brought with it a host of security, privacy and trust challenges for both e-commerce consumers and service providers alike. This conceptual research paper extensively reviews the security, privacy and trust concerns surrounding e-commerce in Kenya and suggests an exhaustive framework for handling the challenges. The research offers appropriate analysis of significant import to academics, policy makers and practitioners in the e-commerce industry in Kenya.

Key words: *e-commerce, security, privacy, trust, ICT, internet, Kenya.*

Introduction and Background to the Study

Since its inception, e-commerce has grown steadily and is now an integral part of day-to-day business activities. However, much as this growth has created various business opportunites, it has also brought with it a host of security, privacy and trust challenges for both e-commerce consumers and service providers alike. It is therefore important for us to understand the key security, privacy and trust issues facing e-commerce in Kenya, where little if any research of this nature has been carried out to date. Accordingly, this paper critically examines the security, privacy and trust issues surrounding e-commerce in Kenya. It subsequently proposes measures to address these three issues.

Definition of E-Commerce

Electronic commerce (E-commerce) has been defined in various ways. For instance, Zwass (1996) defined e-commerce as "the sharing of business information, maintaining business relationships, and conducting business transactions by means of telecommunications networks." Payne (2003) defined electronic commerce as "the exchange of information, conduct of buying and selling, logistics, or other organisational management activities across electronic networks within an organisation, between businesses (B2B), between businesses and consumers (B2C), or between the public and private sectors (B2G), whether paid or unpaid." More recently, the African Union (AU) has described electronic commerce as "all economic activity by which goods and services are offered or provided remotely or by electronic means" (2011). According to the AU, the field of electronic commerce also comprises services such as those providing information online, commercial communications, research tools, access, data retrieval and access to communication or information hosting network, even where such services are not remunerated by the recipients.

Classification of E-commerce

E-commerce has been classified into various categories based upon the entities involved in a transaction. They include business-to-business (B2B), business-to-consumer (B2C), consumer-to-business (C2B), consumer-to-consumer (C2C) and business-to-government (B2G) e-commerce (Bhasker, 2009). B2B is e-commerce carried out between businesses such as between a manufacturer and a wholesaler, or between a wholesaler and a retailer. This is the exchange of products, services, or information between businesses rather than between businesses and consumers. Global B2B transactions comprise 90 per cent of all e-commerce (WTO, 2013). B2C e-commerce entails businesses selling to the general public, typically through catalogues that make use of shopping cart software. Although B2C e-commerce receives a lot of attention, B2B transactions far exceed B2C transactions (WTO, 2013). Consumer-to-business (C2B) can be described as a form of electronic commerce where, the transaction, originated by the customer has a set of requirements specifications and specific price for the commodity, service or item. It is upon the e-commerce entity to match the requirements of the customer to the best possible extent. On the other hand, consumer-to-consumer (C2C) is the e-commerce activity that provides the opportunity for trading of products and/or services amongst consumers who are connected through the internet. This is where individuals transact with each other with the help of an e-commerce platform (Bhasker, 2009). Last but not least, business-to-government (B2G) commerce is generally defined as e-commerce between companies and the public sector. It refers to the use of the internet for public procurement, licensing procedures, and other government related operations (WTO, 2013).

Benefits of E-commerce

E-commerce offers benefits for both businesses and consumers. At firm level, e-commerce has offered numerous opportunities to businesses including reduced transaction and search costs, closer relationships with customers, increased profit and customer loyalty. E-commerce also allows businesses to tailor goods and services to fit the needs of smaller, less affluent consumer bases such as those in developing countries (Mann, Eckert & Knight, 2000). Moreover, e-commerce provides the customer with more choices and customization options by better integrating the design and production processes with the delivery of products and services (Richardson, 2007). The consumer also enjoys a wider choice of products and services at lower prices, as well as certain convenience (no unnecessary trips, no restricted business hours). Because of the interactive nature of e-commerce, an advantage for business produces an advantage for consumers and vice versa, thus contributing to the growth and development of this revolutionary means of exchange. Nonetheless, it is important to note that while e-commerce is generally presented in very positive terms, along with the potential benefits come potential problems (WTO, 2013).

E-commerce in Kenya

According to McKinsey (2013), the internet sector contributed 2.9% of Kenya's GDP. However, this figure should be treated with some caution as accurate statistics of contribution to GDP are hard to come by since in Kenya, ICT (and e-commerce in particular) is not yet considered as a sector in the yearly economic survey reports. Instead, it is classified under 'Transport, Storage and Communications'. It therefore becomes very difficult to track the contribution of ICT to development as a single sector unlike in many countries where ICT is defined as a stand-alone sector. The new Kenya National ICT Master Plan for 2013/14 - 2017/18 recommends that ICT be set up as a stand-alone sector and comprehensive ICT indicators be used to monitor the growth of the sector. Nonetheless, there is a growing consensus that e-commerce in Kenya is destined for rapid growth especially when one considers the growing numbers of online users seeking internet-related services. The growing popularity of e-commerce technology in Kenya presents opportunities for start-ups and established businesses alike (Ghossein, 2013). However, much as this growth in e-commerce adoption and usage has created various business opportunites, it has also brought with it a host of security, privacy and trust challenges for both e-commerce consumers and service providers alike. These issues are addressed in the following sections.

Security, Privacy and Trust Issues surrounding e-Commerce in Kenya

While e-commerce has witnessed tremendous growth in recent years, there are several issues that continue to plague the development of e-commerce globally and Kenya in particular. However, this study will restrict itself to three critical issues for both e-commerce consumers and service providers alike, without which consumers will not visit a website or shop online, nor can e-commerce services function effectively. They are security, privacy, and trust.

Security

In an e-commerce context, security refers to consumers' perceptions about the safety of the online transactions as well as the protection of financial information from unauthorized access (Roman, 2007). Prior studies affirm that security is the most important ethical factor in the online context (Belanger, Hiller & Smith, 2002; Chen & Shergill, 2005; Flavian & Guinaliu, 2006). E-commerce applications such as private e-mail, purchase order processing, transmission of payment information, and workflow automation would be valueless without underlying security infrastructure that makes these exchanges trusted (Ratnasingam, 2002). Unfortunately, security breaches are occurring at a growing rate (Feathermann, Miyazaki & Sprott, 2010). As a result, consumer concerns about the security of Internet transactions continue to be a problem for businesses providing services online as attacks on computer systems are on the rise and the sophistication of these attacks continues to rise to startling levels (Sharma et al., 2009). Further, the sophistication of phishing and pharming scams has increased and affects more unsuspecting web surfers each year (Shin, 2007). Consequently, not only must e-commerce sites and consumers judge security vulnerabilities and assess potential technical solutions, they must also assess, evaluate, and resolve the risks involved (Ackerman & Davies, n.d.).

In Kenya, cyber security is currently a major concern, as recent reports indicate that the country is losing close to 2 billion Kenya shillings annually to cybercrime, necessitating the need to enact appropriate laws that strike a balance between individual rights to privacy and the collective good of the country and its citizens (Ministry of Information, Communications and Technology, 2013). To address this security issue, the government through the CCK established KE-CIRT, the Kenya Computer Incident Response Team Coordination Centre, part-funded by the ITU, which brings together government agencies, the Central Bank and Internet expertise (from KENIC, TESPOK and KENET) to address cyber-attacks as and when they occur (Souter & Kerrets-Makau, 2012). For a long time, the lack of specific cybercrime/cyber security legislation made it difficult to punish those who use ICT tools to commit crime (Murungi, 2011). Therefore, the government has also taken a legal approach; the newly enacted Kenya Information and Communications (Amendment) Act 2014 established the Communications Authority of Kenya to replace the Communications Commission of Kenya. The law has expanded the mandate of the Authority with respect to electronic transactions to include cyber security. Specifically, this mandate entails promoting and facilitating efficient management of critical internet resources and developing a framework for facilitating the investigation and prosecution of cybercrime (CCK, 2014).

Privacy

Culnan (2000) defines privacy as "the ability of an individual to control the terms under which their personal information is acquired and used". According to Sison and Fontrodona (2005), personal information is generally understood to mean any information about an identifiable individual or institution (name, address, telephone number, social security/insurance or other government identification number, employer, credit card number, personal or family financial information, personal or family medical information, etc.). Privacy in e-commerce is defined as consumers' perceptions about the protection of individually identifiable information on the internet (Bart, Shankar, Sultan & Urban, 2005) or the willingness of consumers to share information over the internet (Belanger, Hiller & Smith, 2002). The issue of online privacy protection has gained considerable visibility as consumer advocates, public policy makers, and companies debate the best ways to protect consumer privacy while ensuring that the rights of all stakeholders are protected (Singh & Hill, 2003). One of the key privacy issues in e-commerce concerns the difficulty of securely conveying the information required for online transactions (Suprina, 1997). In particular, financial services providers such

as banks, credit agencies, and payment processors continue to suffer losses of consumers' confidential personal information (Associated Press, 2005). According to Culnan and Armstrong (1999), other major privacy concerns for online consumers relate to unauthorized access to personal data/information as a result of security breaches or the lack of internal controls and the risk of secondary use of their personal data for unrelated purposes without their consent. This includes sharing with third parties who were not part of the transaction in which the consumer related his or her personal data. The information required for online consumer privacy can be breached in through various ways, but mainly through online identity theft as a result of employee abuse, cracking, social engineering, phishing/pharming, spyware/malware and password/login attacks (Newman & McNally, 2005; Chen & Davis, 2006; Sharma, Singh & Sharma, 2009). Spamming (i.e. sending out mass e-mails to consumers who have not requested this information) is also considered unethical.

Increasingly, privacy is considered a complex social phenomenon with interactions among new technologies, regulatory structures, and citizens' perceptions of privacy and social norms (Ackerman & Davis, Jr., n.d.). As a result, some scholars (Reidenberg, 1999; Cranor & Reagle, 1998) have argued that e-commerce privacy requires a combination of law and technology, and Ackerman, Darrell, and Weitzner (2002) have argued that solutions for privacy must simultaneously consider technology, social structures, and regulation in a co-design space. Consequently, governments and other bodies have reacted to growing online consumer privacy concerns by enacting legislation aimed at curbing privacy breaches. For instance, the African Union (AU) has proposed an institutional framework for protection of personal data whereby each member state shall establish an authority with responsibility to protect personal data (AU, 2011). In addition to legislation, new technologies are available to protect user privacy during interactions with Web sites. Many of these tools are used for encrypting e-mail, for making e-mail or surfing activities appear anonymous, for preventing client computers from accepting cookies, or for detecting and eliminating spyware (Laudon, n.d.). Companies in Kenya are also investing in such tools so as to protect the privacy of their customers. Several companies have installed software to counteract e-mail spamming.

Trust

Trust in e-commerce is a belief in the system characteristics, specifically belief in the competence, dependability and security of the system, under conditions of risk (Breaux, James, Parquet & Wright, n.d.). Trust is in an important feature which underpins the use and value of new technologies and therefore can support the development of a digital economy (ICAEW, 2011). Lack of trust in online commercial transactions has been identified as an important barrier to the adoption of e-commerce (Bingi, Mir & Khamala, 2000; Papazafeiropoulou & Pouloudi, 2001; Rotman, 2010). The low level of trust in electronic commerce can be attributed partly to the lack of face-to-face interaction between trading partners in conjunction with the general uncertainty of users in taking advantage of network technologies (Ratnasingham, 1998). To engender trust, e-commerce has tended to look to traditional methods of regulation, such as legislation, international agreements, and voluntary self-regulation (including web site privacy policies and third-party web seals or trust marks) to govern its transactions. While these methods have had success, they do not entirely address unique circumstances or pay sufficient attention to the highly interactive nature of e-commerce transactions (Rotman, 2010).

Analysts argue that the main trouble with online businesses is that Kenyans are yet to trust online shopping. Many Kenyans go online to look for products that cannot be found physically in traditional outlets such as supermarkets, just as a last resort (Nyabiage, 2011). A recent e-commerce study by iHubResearch (2013), also confirmed that Kenyan consumers have low levels of trust in online services. The e-commerce businesses interviewed reported that customers constantly inquire about their existence and/or security of their information, pointing to a lack of trust in the businesses. To address this concern, the CCK is in the final stages of setting up a licensing structure for an authority that will help online buyers verify the authenticity of suppliers. The Regional Certificate Authority (RCA) will link local certification service providers (CSP), bodies authorized by the regulator to issue e- signatures, to its international peers. The lack of a regional certificate authority to authenticate digital signatures provided by other parties across the globe has forced

online buyers of goods and services to depend on international RCAs who offer their services at a higher fee. According to the CCK, the project is part of the Key Public Infrastructure (KPI) information security architecture aimed at boosting the level of Kenyans' confidence and trust in exchanging data through an increasingly insecure Internet. KPI ensures that people are who they say they are and also proves that documents haven't been tampered with, which is critical when conducting online transactions such as placing orders or transferring money. The end result will be to make online or web-based transactions secure and facilitate signing of e-mail or electronic documents to ensure the integrity of their content (Okuttah, 2013).

Conclusion and Implications

Though e-commerce in Kenya is in its formative stages of development, its extraordinary growth over the past years is a clear indication of its enormous potential for conducting business. These new opportunities, however, come accompanied with a large number of concerns and questions that need to be resolved. This article has discussed some of the challenges that face e-commerce consumers, organizations and policy makers in Kenya along three dimensions—security, privacy and trust. It outlines a number of managerial and policy implications that will have to be taken into consideration going forward.

As mentioned, security is a major concern for e-commerce sites and consumers alike. They are an important impediment to expanding e-commerce services and business. Owing to this, consumers need protection against fraudulent, misleading and unfair business practices, and, when things go wrong, to be able to gain redress. Equally, companies need to protect themselves in areas of data integrity, confidentiality, and authenticity of data. It will be necessary to periodically review the regulatory framework so that consumers have effective protection when engaging in electronic commerce. From a legal perspective, the government has done well in enacting the new legislation that upholds consumer online privacy. On their part, e-commerce companies will need to develop and adopt a set of industry standards to protect consumer privacy as a way of supplementing the formal legal obligations. Further, e-commerce businesses can build trust at an individual level by implementing industry best practices, which are underpinned by clear social expectations and legal obligations that are enforceable.

Acknowledgements

This working paper is part of a PhD thesis submitted to the School of Business, Kenyatta University, Kenya.

References

Ackerman, M. S., Darrell, T. & Weitzner, D.J. (2002). Privacy in Context. *Human-Computer Interaction*, 16 (2-4) : 167-176.

Ackerman, M. S. & Davies, Jr. D.T. (n.d.). Privacy and security issues in e-commerce. Review chapter for the New Economy Handbook (Jones, ed.), in press. Retrieved 23/08/2014 from http://econ.ucsb.edu/~doug/245a/Papers/ECommerce%20Privacy.pdf

African Union (2011). *Draft African Union convention on the establishment of a credible legal framework for cyber security in Africa*. Retrieved 23/05/2014 from http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/events/2011/WDOcs/CA_5/Draft%20Convention%20on%20Cyberlegislation%20in%20Africa%20Draft0.pdf

Breaux, D., James, J., Parquet, K. & Wright, A. (n.d.). *Trust in e-commerce*. Retrieved 05/09/2014 from http://apwright.weebly.com/files/theme/eCommerce.pdf

Samtani, A. (2001). Electronic commerce in Asia: the legal, regulatory and policy issues. *International Journal of Law and Information Technology*, 9(2), 93 – 114.

Bart, Y., Shankar, V., Sultan, F. & Urban, G.L. (2005). Are the drivers and role of online trust the same for all websites and consumers? A large-scale exploratory empirical study. *Journal of Marketing*, 69 (4), 133-52.

Belanger, F., Hiller, J. S. & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes, *Journal of Strategic Information Systems*, 11(3/4), 245-70.

Bhasker, B. (2009). *Electronic Commerce: frameworks, technologies and applications*. New Delhi: Tata-McGraw-Hill.

Bingi, P., Mir, A. & Khamalah, J. (2000). The challenges facing global e-commerce, *Information Systems Management*, 17:4, 22-30, DOI: 10.1201/1078/43193.17.4.20000901/31249.5

Chen, Z. & Shergill, G. S. (2005). Web-based shopping: consumers' attitudes towards online shopping in New Zealand. *Journal of Electronic Commerce Research*, 6(2), 79-94.

Communications Commission of Kenya (2014). Key changes in the ICT sector law. Retrieved 23/05/2014 from http://www.cck.go.ke/links/public_notices/2014/Changes_ICTsector_Law.pdf

Cranor, L., & Reagle, R. (1998). The Platform for Privacy Preferences. *Communications of the ACM*, 42 (2) : 48-55.

Creed, A., Zutshi, A. & Ross, J. (2009). Relational ethics in global commerce. *Journal of Electronic Commerce in Organizations*, 7 (1), 35–49.

Culnan, M. J. (2000). Protecting Privacy Online: Is Self-Regulation Working? *Journal of Public Policy and Marketing*, 19 (1): 20-26.

Culnan, M. J. & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation. *Organization Science*, 10 (1), 104-115.

European Commission (2011). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: a renewed EU strategy 2011-14 for Corporate Social Responsibility*. Accessed 14/06/2014 from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0681:FIN:EN:PDF

Featherman, M.S., Miyazaki, A. D. & Sprott, D. E. (2010). Reducing online privacy risk to facilitate e-service adoption: the influence of perceived ease of use and corporate credibility. *Journal of Services Marketing*, 24(3), 219–229.

Flavian, C. & Guinaliu, M. (2006). Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a website, *Industrial Management & Data Systems*, 106 (5), 601-20.

Frynas, J. G. (2002). The limits of globalization – legal and political issues in e-commerce. *Management decision*, 40 (9), 871 – 880.

Ghossein, M. (2013, April 25). Internet the conduit to a digital economy. *Business Daily*. Accessed 12/06/2014 from http://www.businessdailyafrica.com/Opinion-and-Analysis/Internet-the-conduit-to-a-digital-economy/-/539548/1758200/-/dwc4lv/-/index.html

Hargreaves, D. (1999, October 29). Clash looms on e-commerce regulation. *Financial Times*.

Forcht, K.A. & Wex, R-A. (1996). Doing business on the Internet: marketing and security aspects, *Information Management & Computer Security*, 4(4), 3-9.

Institute of Chartered Accountants in England and Wales (2011). Building trust in the digital age: rethinking privacy, property and security. *Making Information Systems Work Initiative*. Retrieved 19/05/2014 from http://www.icaew.com/~/media/archive/files/technical/information-technology/business-systems-and-software-selection/making-information-systems-work/building-trust-in-the-digital-age-report.pdf

iHubResearch (2013). E-commerce research report: An exploratory study on e-commerce in Kenya, Uganda and Tanzania. *Afrikoin Conference Report*. Accessed on 02/06/2014 from http://www.mbuguanjihia.com/downloads/AfricoinReportpdf2014-2-6-13-57-16.pdf

Kenya ICT Authority (2014). *Kenya National ICT Master Plan for 2013/14 - 2017/18*. Accessed 12/06/2014 from https://www.kenet.or.ke/sites/default/files/Final%20ICT%20Masterplan%20Apr%202014.pdf

Laudon, K.C., Traver, C.G. & Laudon J.P. (1996). *Information Technology and Society*, p.513.

Mann, C.L., Eckert, S.E. & Knight, S.C. (2000). *Global electronic commerce: A policy primer*. Washington, DC: Institute for International Economics.

Maury, M. D. & Kleiner, D. S. (2002). E-commerce, ethical commerce? *Journal of Business Ethics*, 36 (1/2), 21–31.

McCune, J.C. (1999). Big brother is watching you. *Management Review*, 88(3), 10-12.

McKinsey (2011). Internet matters: The net's sweeping impact on growth, jobs and prosperity. *Report by McKinsey Global Institute*. Accessed 22/05/2014 from http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Internet_matters.

Ministry of Information, Communications and Technology (2013). *Remarks by ICT Cabinet Secretary Dr.Fred Matiangi while addressing the press during the Information security and Public Key Infrastructure Conference in Nairobi, Kenya*. Retrieved 22/05/2014 from http://www.information.go.ke/?p=241

Murungi, M. (2011). *Cyber Law in Kenya*. Alphen aan de Rijn: Kluwer Law International.

Newman, R. G., & McNally, M. M. (2005). *Identity theft literature review*. Accessed 04/09/2010 from http://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf.

Nyabiage, J. (2011, October 26). E-commerce blow to Kenya as Kalahari site shuts down. *The Standard*. Accessed 02/06/2014 from http://www.standardmedia.co.ke/business/article/2000045622/e-commerce-blow-to-kenya-as-kalahari-site-shuts-down

Okuttah, M. (2013, February 13). CCK moves closer to setting up system for online commerce. *Business Daily*. Accessed on 12/06/2014 from http://www.businessdailyafrica.com/-/1248928/1693126/-/14j308cz/-/index.html

Papazafeiropoulou, A. & Pouloudi, A. (2001). Social issues in electronic commerce: Implications for policy makers. *Information resources management journal*. 14 (4).

Ratnasingham, P. (1998). The importance of trust in electronic commerce. *Internet Research: Electronic Networking Applications and Policy*, 8(4), 313-321.

Ratnasingam, P. (2002). The importance of trust in web services security. *Information Management & Computer Security*, 10 (5), 255–260.

Reidenberg, J. R. (1999). Restoring Americans' Privacy in Electronic Commerce. *Berkeley Technology Law Journal*, 14 (2) : 771-792.

Richardson, (2007). Current issues in marketing in the information age (2nd Ed).

Rotman, L. I. (2010). Trust, loyalty and e-commerce. In D. E. Palmer (Ed). *Ethical issues in e-business: models and frameworks* (pp. 58 – 79). Hershey, PA: IGI Global.

Sharma, K., Singh, A. & Sharma, V. P. (2009). SMEs and cyber security threats in e-commerce. *EDPACS: The EDP Audit, Control, and Security Newsletter*, 39(5-6), 1-49.

Shin, A. (2007, February 10). *Taking the bait on a phish scam: job seekers are targets, victims of sophisticated ploy*. Washington Post. Accessed from www.washingtonpost.com/wp dyn/content/article/2007/02/09/AR2007020901925.html.

Singh, T. & Hill, M. E. (2003). Consumer privacy and the Internet in Europe: a view from Germany. *Journal of Consumer Marketing*. 20 (7), 634 – 651.

Sison, A. J. & Fontrodona, J. (2005). Ethical aspects of e-commerce: Data subjects and content. Working Paper 586, University of Navarra – IESE Business School,

Souter, D. & Kerrets-Makau, M. (2012). Internet governance in Kenya – an assessment for the internet society. *ICT Development Associates Limited*. Accessed 21/05/2014 from http://www.internetsociety.org/sites/default/files/ISOC%20study%20of%20IG%20in%20Kenya%20-%20D%20Souter%20%26%20M%20Kerretts-Makau%20-%20final.pdf

Suprina, D. (1997). Privacy, identity and non-refutability: Requirements for digital age applications. *Sun Journal*, 1- 3.

World Trade Organization (2013). *E-Commerce in developing countries: Opportunities and challenges for small and medium enterprises*. Accessed on 02/06/2014 from www.wto.org/english/res_e/publications_e/ecom_devel_countries_e.htm

Zwass, V. (1996). Electronic commerce: Structure and issues. *International Journal of Electronic Commerce*, 1(1), 3-23.

Authors' Details

Peter Misiani Mwencha	PhD Candidate, Kenyatta University, Nairobi, Kenya. E-mail: mwencha@hotmail.com
Stephen Makau Muathe	PhD, Lecturer, Kenyatta University, Nairobi, Kenya. E-mal: muathesm@yahoo.com
John Kuria Thuo	PhD, Associate Professor, Gretsa University, Thika, Kenya. E-mail: thuokuria@yahoo.com