ASSESSMENT OF SECURITY MEASURES IN UNIVERSITIES FOR ENFORCEMENT OF INTEGRITY OF INFORMATION SYSTEMS IN KISUMU AND SIAYA COUNTIES, KENYA

Martin M. N. Musyoka, George Raburu, and Castro Yoga
School of Informatics and Innovative Systems
Jaramogi Oginga Odinga University of Science and Technology
P.O. Box 210-40601, BONDO-Kenya

N. B. Okelo
School of Mathematics and Actuarial Science
Jaramogi Oginga Odinga University Science and Technology
P.O. Box 210-40601, BONDO-Kenya

ABSTRACT

An ICT policy safeguards Integrity of Information Systems and ensures business continuity. This study sought to assess the level of compliance by Universities to their ICT security policies by assessing the integrity pillar. Literature review on Integrity of Information Systems as well as international standards and regulations such as HIPAA, FERPA, SOX and ISO 270003 that touch on CIA was carried out. A cross-sectional survey study design incorporated self-administered quantitative and qualitative research that was carried out in eight campuses within Kisumu and Siaya Counties. The survey was conducted on universities that gave authorization of the survey to go on. Stratified sampling method was used to arrive at the right population of respondents in the universities. The study targeted ten campuses within the two counties but only eight authorized the study. The findings of this study reveals that overall compliance ratings in the three key pillars of IT security were below 50% on compliance ratings with integrity at 30% This study contributes to policy, practice and theory at county and individual level in two ways. Firstly it came up with empirical data on state of compliance to ICT policies in universities and secondly it will provide the government and the institutions' management with an objective profile of issues and a proactive approach that can solve the issues in cost effective manner.

INTRODUCTION

Institutions of higher learning have a unique organizational environment mainly due to the need for the principle of academic or intellectual freedom. Academic freedom entails the freedom of teachers and students to teach, study, and pursue knowledge and research without unreasonable interference or restriction from law, institutional regulations or public pressure. Kambwiri (2012) observes that the issue of censorship should not rise because of national and international legislation already makes some resources illegal. Court cases have in the past being fronted to challenge academic freedom such as Urofsky v. Gilmore (1999) and Sweezy v. New Hampshire (1957) (Kim, 2005). Distrust and suspicion impedes scholarly work and thus need to have academic freedom (Kambwiri, 2012).

Just as business entities put in place measures to protect sensitive information, higher institutions of learning have the same requirements regardless of the need for open access and principles of academic/intellectual freedom, (Beaver, 2010). Skilled hackers have realized Higher Education institutions have some of the richest deposits of identity data (Oracle, 2008). Such information may include Social Security Numbers, bank accounts for students, detailed information about students and staff. The "openness" of campus networks makes it easy to facilitate and collaborate information across researchers and students. This architectural design which 'Unlike private corporate networks, which, by their nature are designed to be "walled gardens" of information, leave campus networks more vulnerable to misuse and attacks (Kambwiri, 2012). Research by Oblinger (2003) indeed collaborates this theory, 'the instructional and research environment of colleges and universities are more pervasive and open than in government and corporate training departments and research laboratories.' As much as higher education environment reasons has a strong need for open and accessible networks, it has an obligation on the part of each college to protect the systems and data they contain (Kambwiri, 2012). Higher Education is faced with 'the need to apply appropriate security without compromising the fundamental principles of the academia' (Oblinger, 2003:1). Educators may agree with the need for security, differences of opinion arise when specific practices are proposed; for instance technology staff may view use of firewall as a necessary precaution while faculty may see it as a restriction or an impediment to intellectual freedom. Need for decentralized research space in the academia to promote education and research has often been exploited by hackers thus the increased IT security incidences.'The academic culture tends to favor experimentation, tolerance and individual autonomy – all characteristics that make it more difficult to create a culture of computer and network security' (Oblinger, 2003:3). Indeed the nature of higher education is to foster an open academic environment, which is a nature at odds with the need to protect sensitive information and be mindful of security issues (Application Security Inc., 2010). As a result, as Bates (2011:1) puts it, 'security standards and controls are nearly an abomination to academia.'

Beaver (2010) observes that information risks at campuses are from multiple angles which include websites, student information systems (front-end web applications, backend databases, and servers), weakly configured wireless networks, laptops, and other mobile devices such as smart phones, ipads, netbooks, and USB thumb drives. Indeed high speed wireless computing is creating a new breed of College and University students (Motorola, 2009). NEC (2005) cites the increase of e-mail use, distance learning, and other services that enhance the quality of student experience and extend education beyond the campus as having a potentially significant privacy price if not well managed. Bates (2011) complains that information security in higher education has continued to develop in an ad hoc manner or reactive mode, perhaps more than in any other sector. A few distinct risks associated with the higher education market's IT infrastructure include open access terminals that are on the same network as sensitive databases, high student population and turnover, decentralized IT sections within one campus, and budgetary constraints (Application Security Inc., 2010). Bates (2011) states that the academia faces an ever changing information security landscape with respect to threats, emerging technologies, vulnerabilities, and compliance standards and that mobile devices arriving on campus in great numbers (through students) challenge controlled data access.

At least half of the breaches to information security systems are carried out by internal users and mainly involve unauthorized system access. But there is also a positive side of users. A study by Kambwiri (2012) in Spears et al (2010) reveals that internal users can complement value to IS security when they are involved in the prioritization, analysis, design, implementation, testing, and monitoring of user –related security controls in the business process. Oracle (2008) concludes that ‘having fewer safeguards to protect identity due to their organizational structure, less available budget, and a population less aware of identity theft risks make universities more attractive to crime. Beaver (2010) points out that the first and foremost information security challenge in higher education is limited budgets that leads to use of freeware and open source tools to perform tasks that require commercial solutions. According to Kambwiri (2012) in Application Security Inc. (2010), budgetary constraints represent perhaps the most rational reason why colleges and universities are experiencing a high volume of attacks. He continues to add that University IT departments are often plagued by resource issues, disparate database systems and potentially numerous IT departments with budgetary constraints. NEC (2005) observes that with respect to capital constraints, many institutions have allocated the responsibility of information security to all IT staff, effectively making it everyone’s responsibility, an ineffective approach due to lack of ownership. Outdated or missing malware protection, unenforced e-mail encryption, use of pirated softwares and lack of preventive controls for data loss are some of the biggest mistakes regarding information security in higher education. Another challenge though, according to Beaver (2010), is cultural adaptation to academic information security management since academic departments utilize IT differently.

CONCEPTUAL FRAMEWORK

The conceptual framework in fig 2 below was used to make conceptual distinctions and organize ideas thus providing direction for the research work.

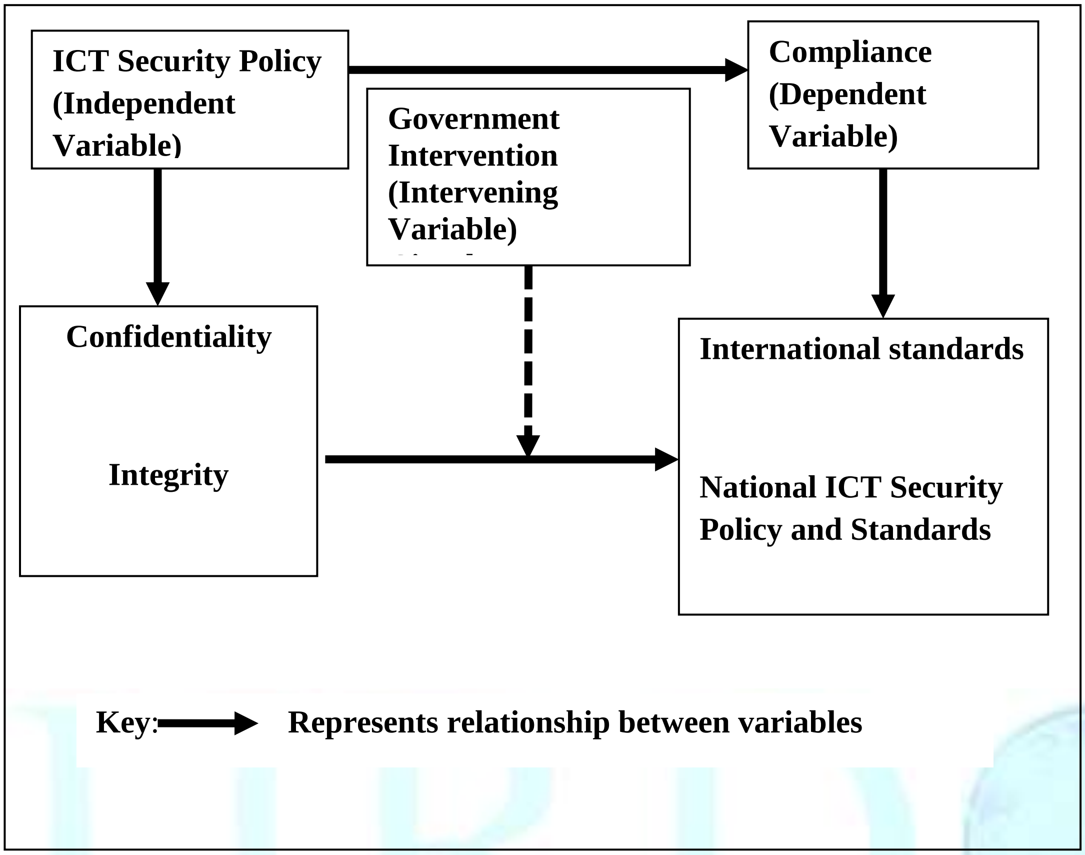
ICT Security Policy (Independent Variable)
Government Intervention (Intervening Variable)
Compliance (Dependent Variable)
Confidentiality
Integrity
International standards
National ICT Security Policy and Standards
Key:
Represents relationship between variables

Fig 1: Interaction between the variables under conceptual Framework

From the framework, the independent variable is the factor that is measured, manipulated or selected by the researcher to determine its relationship to compliance, it may be called factor and its variation called levels. It is presumed to cause changes to occur in another variable hence causal variable (Kenny and Baron, 1986). Therefore, the independent variable is ICT security policy broken down into three levels: Confidentiality, Integrity and Availability of ICT systems and infrastructure that could affect compliance.

The intervening variable is a variable that comes in between other variables. It helps to delineate the process through which variables affect one another hence it is one that links between the independent variable and dependent variable (Kenny and Baron, 1986). The government at times issues directives through circulars through the Communications Commission of Kenya on National ICT policy, as well as matters affecting IT security at the national scene. The ministry of health may on the other hand, issue guidelines that must be followed when doing research especially how to disseminate such information. This in itself may make institutions comply to their own ICT policies, in regards to confidentiality, and privacy of data and hence contribute to compliance to the National ICT policy as well as legal requirements. The researcher assumes that any directive from the government is acted upon by all institutions.

The dependent variable is a variable that changes because of another variable hence it is the effect or the outcome variable (Kenny and Baron, 1986). By selecting the three pillars of IT Security aka CIA which are derived from ICT security policy, the researcher is able find out how compliance is achieved in terms of National ICT policy, disaster recovery and business continuity, and compliance to legal and regulatory framework.

RESULTS AND DISCUSSIONS

The study sought to examine security measures put in place in universities to enforce integrity of information systems. The following table (table 6) provides a summary of Information systems Integrity questions with aggregated frequencies with the following columns/labels: "Yes", "No" & "Don't Know" that were asked to the respondents.

Table 6: Measures enforcing Integrity

Information Systems Integrity questions	**Yes** **Freq (%)**	**No** **Freq (%)**	**Don't Know** **Freq (%)**
Have you ever lost your data or had data breach?	168(50.6)	141(42.5)	23(6.9)
Do you believe your information systems are secure enough?	123(37.4)	137(41.6)	69(21.0)
Is there any existing control against malicious software usage?	166(50.2)	48(14.5)	117(35.4)
Is automatic computer screen locking facility enabled in the computer you work on?	149(44.8)	142(42.8)	41(12.4)
Is there any procedure that exists to verify that all warning bulletins are accurate and informative with regard to malicious software usage?	143(43.3)	74(22.4)	113(34.2)
Are you prohibited to use of unauthorized or pirated software or unlicensed software in the institution?	204(62.2)	72(22.0)	52(15.9)
Do you receive unnecessary emails from people you even don't know (spam mails) through the official mail?	182(55.5)	116(35.4)	30(9.2)
Is the information security policy communicated to all employees on an ongoing basis?	130(39.4)	113(34.2)	87(25.4)
Do you believe employees continue to access online services via internet such as ERP even after employment has	110(33.7)	87(26.7)	129(39.6)

been terminated?			
Average score (%)	46	32	22

From the table above, half of the total respondents reported to have lost data or had data breach, 141(42.5%) of them had not lost data or had data breach, while 23(6.9%) of them did not know whether they had lost any data or had data breach or not.

Most of the respondents did not believe that their information systems are secure enough at the campuses that were interviewed. 138(41.6%)disagreed versus 124(37.4%) agreed while 70(21%) of them did not know. Half of the respondents agreed that there exists some controls against malicious software usage, 48(14.5%) of them disagreed that there existed any controls against malicious software usage, while more than a third did not know.

Automatic computer screen locking facility as a first step to information integrity and security is implemented at a 50-50 basis. More or less similar proportions of respondents agreed and also disagreed that there existed an automatic computer screen locking facility enabled in the computers they worked on. However 41(12.4%) of them did not know whether there was an automatic computer screen locking facility enabled in the computers they worked on or not.

Close to half of the respondents at 144(43.3%) agreed that there existed some procedures to verify that all warning bulletins are accurate and informative with regard to malicious software usage, 114(34.2%) disagreed that there existed any procedures to verify that all warning bulletins are accurate and informative with regard to malicious software usage while about a third of them 113(34.2%) did not know.

206(62.2%) of the respondents agreed that they are prohibited to use of unauthorized or pirated software or unlicensed software in the institution, 73(22%) of the disagreed that they are prohibited to use of unauthorized or pirated software or unlicensed software in the institution, while 53(15.9%) did not know whether they are prohibited to use unauthorized or pirated software or unlicensed software in the institution or not.

More than half 184(55.5%) of the respondents in this study agreed that they received unnecessary emails from people they didn’t know (spam mails) through the official mail, 117(35.4%) of them disagreed that they received unnecessary emails from people they didn’t know (spam mails) through the official mail, while 31(9.2%) of them did not.

A higher proportion of the respondents 132(39.6%) didn’t know if they believed or not that employees continued to access online services via internet such as ERP even after employment has been terminated, a third of the respondents 86(26.7%) disagreed that employees continued to access online services via internet such as ERP even after employment has been terminated while 112(33.7%) of the respondents believed that employees continued to access online services even after employment has been terminated.

With an overall percentage of 46%, integrity was found to be with the least score. This implies that most systems maybe at a great risk in terms of Integrity. Issues of records manipulation, altered grades or falsified financial records are as a result of lack of enough measures enforcing integrity of information systems and may be experienced in near future if institutions connect to high speed networks where hackers for hire are paid to exploit systems weaknesses.

CONCLUSION

.Data analysis and interpretation revealed that majority of the information systems lack integrity. With overall score of 46%, it’s a pathetic situation. When the integrity of information systems is highly compromised, it casts doubts on the data/information produced by the same systems. Enhancing data Integrity measures will improve the data quality.

REFERENCES

Andress, J. (2011) The Basics of Information Security: Understanding the Fundamentals of Information Security in Theory and Practice, USA: Elsevier.

Application Security, Inc. (2010) ‘An Examination of Database Breaches at Higher EducationInstitutions’. Retrieved July 11th, 2012 from http://www.appsecinc.com/techdocs/whitepapers/Higher-Ed-Whitepaper-Edited.pdf.

Anonymous (2012, November 7)IT Security Breach News Roundup: ‘Team Ghostshell’ Targets Top Universities While S.C. and B&N Suffer Big Breaches. Retrieved from http://blogs.carouselindustries.com/security/it-security-security/it-security-breach-news-roundup-team-ghostshell-targets-top-universities-while-s-c-and-bn-suffer-big-breaches/

Anonymous (2012, November 7) Carausel Connect. Retrieved November 7, 2012 from http://blogs.carouselindustries.com/security/it-security-security/it-security-breach-news-roundup-team-ghostshell-targets-top-universities-while-s-c-and-bn-suffer-big-breaches/ on.

Anonymous (2000) Personal Data Protection Act (Unofficial translation). Retrieved from http://www.dutchdpa.nl/downloads_wetten/wbp.pdf?refer=true.

Appliedtrust (n.d) Information Security. Retrieved July 1st, 2013 from http://www.appliedtrust.com/sites/default/files/assets/resources/figure1.png

Azevedo A. (2012, October 3), Hacker Group Breaches Thousands of University Records to Protest Higher Education. Retrieved from http://chronicle.com/blogs/wiredcampus/category/security

Bates, C. (2011) ‘Taking Your Information Security Program to the Next Level: a Higher Education Perspective’, University of Arizona. Retrieved from http://iasec.eller.arizona.edu/docs/whitepepers/take_info_security_to_next_level.pdf.

Beaver, K.(2010), Information Security in Higher Education Sophos. USA: Boston. Retrieved from http://www.sophos.com/sophos/docs/eng/factshts/sophos-information-security-higher-education-ssna.pdf

Braud, L. (2010, January 4). *Sample size and Population*. UNU.edu: Sample Size and population Definition. Retrieved March 14,2011from http://www.unu.edu/unupress/unupbooks

BSI (2005) BS ISO/IEC 27002:2005 - Information technology. Security techniques. Code of practice for information security management. London, UK: BSI.

Council of Europe (1950) European Convention for the Protection of Human Rights and Fundamental Freedoms. Retrieved from http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm.

Council of Europe (1981a) Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data. Retrieved from: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

Council of Europe (1981b) Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data - Explanatory Report. Retrieved from: http://conventions.coe.int/treaty/en/Reports/Html/108.htm.

Carousel Inc. (2012, November 7). Carousel Connect. Retrieved from http://blogs.carouselindustries.com/security/it-security-security/it-security-breach-news-roundup-team-ghostshell-targets-top-universities-while-s-c-and-bn-suffer-big-breaches/

European Council, European Parliament & Commission on the Charter of Fundamental Rights (2000) Charter of Fundamental Rights of the European Union. Retrieved from http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

European Data Protection Supervisor (2013, November 10). The European guardian of personal data protection. Retrieved from: http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/20

Fischman, J. (2008, march 13) Harvard Security Breach Exposes Sensitive Student Data .*The Chronicle*. Retrieved from http://chronicle.com/blogs/wiredcampus/harvard-security-breach-exposes-sensitive-student-data/3758

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The Qualitative Report, 8(4)*, 597-607. Retrieved from http://www.nova.edu/ssss/QR/QR8-4/golafshani.pdf

Grobler, C. &Louwrens, C. (2007) 'Digital Forensic Readiness as a Component of Information Security Best Practice'. In, New Approaches for Security, Privacy and Trust in Complex Environments. pp. 13-24.

Höne, K. &Eloff, J.H.P. (2002) 'Information security policy -- what do international information security standards say?' Computers & Security, 21 (5), pp. 402-409.

House of Representatives (2002) Sarbanes-Oxley Act.Conference Report. Retrieved August 29, 2014 from *www.ucema.edu.ar/cegopp-base/download/LeydeSarbanes.pdf*

Information Security Forum Limited (2007) The Standard of Good Practice for Information Security. London, UK: ISF.

International Labour Office Geneva (1997) Protection of workers' personal data. Retrieved from http://www.ilo.org/public/english/protection/safework/cops/english/download/e000011.pdf.

International Organization on Computer Evidence (IOCE) (2002) Guidelines for Best Practice in the Forensic Examination of Digital Technology. Retrieved from: http://www.ioce.org/fileadmin/user_upload/2002/ioce_bp_exam_digit_tech.html#G8Principles.

IT Governance Institute (2007) COBIT 4.1. Rolling Meadows, IL, USA: IT Governance Institute.

Kambwiri, L. M. (2012). *An Appraisal of Information Security Management at Chancellor College, University of Malawi* (Published master’s thesis).LuleåUniversity of Technology, Lulea, Sweden. Retrieved from https://pure.ltu.se/ws/files/41120951/LTU-EX-2012-40162171.pdf

Kenny, D.A. and Baron, R.M. (1986). "*The Moderator-Mediator Variable Distinction in Social Psychological Research*: Conceptual, Strategic, and Statistical Considerations. "*Journal of Personality and Social Psychology*

Kenyan Constitution.(2010) Privacy.Bill of Rights, Part 2—Rights and fundamental freedoms, Article 31.p 28.

Kerlinger, F.N. (1969). *Research in Education*.In R. Ebel, V. Noll, & R. Bauer (Eds.), Encyclopaedia of Education 4th edition. New York: Macmillan.

Kim, E. (2005) Academic Freedom on the Internet. Unpublished Thesis (PhD), University of Illinois.

Kombo, D.K. and Tromp, D.L.A. (2006).*Proposal and Thesis writing*: An introduction. Pauline Publications African, Nairobi.

Kothari, C.R. (1990). *Research methodology book*, 2nd edition, pages 32-39 & 98, 100 & 101.

Krejcie, R.V., & Morgan, D.W., (1970). Determining Sample Size for Research Activities.*Educational and Psychological Measurement*

Mandol, P. S. (2004). Formulation of IT Auditing Standards. Paper presented at an IT Audit Seminar, National Audit Office, China. Retrieved from www.cnao.gov.cn/UploadFile/NewFile/2006612113459150.doc.

Mattord, H. & Whitman, M. (2011) Principles of Information Security, 4th edition, Boston: Course Technology.

Mbuvi, D. (2013) Google, Microsoft, Linkedin Hacked in Kenyan DNS Hijack. Retrieved from http://allafrica.com/stories/201304152114.html

Mitrou, L. &Karyda, M. (2006) 'Employees' privacy vs. employers' security: Can they be balanced?' Telematics and Informatics, 23 (3), pp. 164-178.

Motorola (2009) Motorola’s Higher Education Solutions: Indoor and Outdoor Connectivity. Retrieved from http://wirelessnetworkchannel-asia.motorola.com/ pdf/sm_vertical_market_segment_sales tools/education/Higher%20Ed%20Brochure.pdf.

Mugenda, A.G. (2008). *Social Science Research theories and Principles*, Kijabi printing press, Nairobi.

Mugenda, O.M. and Mugenda, A.G. (1999).*Research methods: Quantitative and Qualitative Approaches*: Nairobi: ACTS Press.

NEC Unified Solutions, Inc (2005) Information Security: A Perspective for Higher Education. Retrieved July 07, 2012 fromhttp://www.necunified.com/Downloads/WhitePapers/ NEC_HigherEd_InformationSecurityWhitePpr.pdf.

NIST.gov - Computer Security Division - Computer Security Resource Center (2006) NIST's Policy on Hash Functions. Retrieved from: http://csrc.nist.gov/groups/ST/hash/policy.html.

NIST.gov - Computer Security Division - Computer Security Resource Center (2009) NIST Special Publications 800 series. Retrieved from: http://csrc.nist.gov/publications/PubsSPs.html.

NIST.gov - Guide for Mapping Types of Information and Information Systems to Security Categories (2008) NIST Special Publication 800-60 Volume I Revision 1 [Online]. Retrieved from: http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf

Oblinger, D. (2003). “Computer and Network Security and Higher Education’s Core Values.” EducauseCenter for Applied Research, Vol. 2003, No. 3.

Oblinger, D. (2003) ‘IT Security and Academic Values’, London: Jossey-Bass. Retrieved from http://net.educause.edu/ir/library/pdf/pub7008e.pdf.

Office of Consumer Affairs and Business Regulation (n.d.) 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth. Retrieved from www.mass.gov/Eoca/docs/idtheft/201CMR17amended.pdf.

Onwubiko, C. (2009). A Security Audit Framework for Security Management in the Enterprise. . Retrieved from http://www.springerlink.com/content/v12786838l8046h3/.

Omaha, N. (2012, May 25) University of Nebraska reports major security breach. Retrieved from http://www.ketv.com/news/local-news/University-of-Nebraska-reports-major-security-breach/-/9674510/14230812/-/2hjt7f/-/index.html#ixzz2DQfxcsWT

Oracle (2008) ‘How Secure is Higher Ed?’. FOCUS. Retrieved fromhttp://www.oracle.com/us/industries/045694.pdf.

Oso, W. &Onen, D. (Eds.). (2008*) A general guide to writing research proposal and report.* A handbook for beginning researches (2nd Ed.).(pp.85-99).Makerere University, Kampala.

Santos, H., & Pereira, T. (2010).Conceptual Framework to Manage and Audit Information Systems Security.

Sofie, P. &. (2010). *Information Security as a Pre-requisite for e-Government Services - Developing the Organizations and the Information Systems.* Proceedings of the 6th International Conference on e-government. NR Reading England: ACADEMI.

Techtarget (n.d.) Confidentiality, Integrity and Availability. Retrieved March 22, 2015 from http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA.

The Times(2010) The Times Of India.Retrieved July 15, 2013 fromhttp://timesofindia.indiatimes.com/topic/KU-website-hacked

Ranjan, J. (2008) ‘Impact of Information Technology in Academia’, International Journal of Educational Management, Vol. 22, No. 5, pp 442-455.

United Nations (1948) the Universal Declaration of Human Rights. Retrieved February 6, 2009 from: http://www.un.org/Overview/rights.html

William,K. (2006). "Descriptive Statistics".*Research Methods Knowledge Base*. http://www.socialresearchmethods.net/kb/statdesc.php.

Wessa P., (2008), Pearson Correlation (v1.0.3) in Free Statistics Software (v1.1.23-r6), Office for Research Development and Education, URL http://www.wessa.net/rwasp_correlation.wasp/