CONFIDENTIALITY AND AVAILABILITY OF SECURITY MEASURES FOR INFORMATION SYSTEMS IN UNIVERSITIES 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

Many organizations continue to grow in numbers by the day in adopting use and adoption of ICT in day to day business processes and so are the rising trends in cyber insecurity. Securing information systems against myriad spectrum of threats requires use of multiple, overlapping protection approaches addressing people, technology and operational processes. ICT policies are put in place in institutions to provide guidelines and standards on what is acceptable and what is not as regards to use of ICT systems. In spite of these ICT policies, numerous instances all over the world have been reported whereby university systems were compromised and university information exposed to other third parties or malicious activities or unintentional errors. According to a report published by Oracle (2008), there have been hundreds of data breaches costing millions of dollars and damaging universities' reputation. There is no evidence that research has been carried out in the past to assess the level of compliance to ICT security policies by the institutions of higher learning. This study therefore sought to bridge this gap by means of a survey, to investigate and describe the level of compliance to ICT security policies in terms of confidentiality and availability in Universities in Kisumu and Siaya Counties, Kenya.

INTRODUCTION

Information security policy major role in organizations is to address threats. Policies and procedures define the organizations' guiding principles, often by providing detailed task instructions and performing basic structure for critical business operations of the organization. The services and operations of today's organizations are increasingly dependent on their information systems (IS) that are supported by computer and internet technologies. As a result, organizations' operations have already been changed from traditional information systems to computer based information systems. These systems help students and staff alike to access university resources anytime, anywhere. Universities are increasingly relying on Information Technology(IT) systems for essential business operations, including administration, teaching, learning, and research. Applying information security to university IT systems and information is strategically important to maintain overall business continuity.For institutions to provide secure IT infrastructure, they need to adequately address the issue of IT Security(Sofie, 2010). Lack of sufficient IT security can negatively affect performance of institutions.

The main objective of ICT Security policy is to ensure smooth operations and minimize damage or destruction, protect the interests of parties that depend on information systems from the effects of failure or weakness of confidentiality, integrity, availability, validity information and communication. Although implementing information security in universities is an important function, it is not always given priority as many universities and colleges focus on the core business which is dissemination of knowledge and research. A survey is an important tool to assess the level of compliance to ICT security policy in institutions with in a very challenging environment where competing priorities exist.

RESULTS AND DISCUSSIONS

Security measures put in place in universities to enforce confidentiality of information systems

The study sought to know security measures put in place in universities to enforce confidentiality of information systems. Table 4 below shows the frequencies of measures enforcing Confidentiality of Information Systems with "Yes", "No" and "Don't Know" columns aggregates.

Table 5:Measures enforcing Confidentiality of information systems

Information Systems Confidentiality questions	**Yes Freq (%)**	**No Freq (%)**	**Don't Know Freq (%)**
Do you have an information security policy in your college/university	203(61.1)	31(9.3)	98(29.5)
Do your password expire in every three months and force you to change them	126(38.0)	162(48.8)	44(13.23)
Do you report any data or security breach	212(67.3)	81(25.7)	22(7.0)
Did you sign a confidentiality statement or form upon employment	206(63.0)	89(27.2)	32(9.8)
Have you ever attended data security workshop or training facilitated by the institution in the last 3 years	186(56.9)	117(35.9)	24(7.3)
Is there a formal disciplinary process in place for employees who have violated organizational security policies and procedures	185(55.7)	49(14.8)	98(29.5)
Is the information security policy communicated to all employees on an ongoing basis	146(44.0)	90(27.1)	96(28.9)
Are you aware of any spot checks or regular audits conducted by the ICT department to make sure staff access to electronic resources are not compromised by third party like hackers	148(44.6)	105(31.6)	79(23.8)
Were you as a staff involved in the development of the ICT security policy	119(36.3)	172(52.4)	37(11.3)
Average score (%)	51.9	30.3	17.8

From the table above more than half of the respondents agreed that there was information security policy in the universities within the two counties. Out of 332 respondents 31(9.3%) of the respondents disagreed that there was information security policy in the universities within two countieswhile 98(29.5%) of them did not know whether there was or not information security policy in the universities. Also more than half at 173(52.4%) of the respondents disagreed to be involved in the development of the ICT security policy, 120(36.3%) of them said that they were involved in the development of the ICT security policy, while 36(11.3%) of them did not know whether they were involved in the development of the ICT security policy or not.

Close to half 159(48.8%) of the respondents disagreed that their information systems login passwords expired in every three months and forced to change the passwords. 126(38%) of them agreed that their passwords would expire in every three months and forcedthem to change their passwords while 44(13.2%) of them did not know. Most of the respondents 223(67.3%) said they reported data or security breach encountered in their workstations, 85(25.7%) said that they did not report any data or security breach while 23(7%) of the total respondents did not know whether they reported or not.

Majority of the respondents agreed that they signed a confidentiality statement or form upon employment, 89(27.2%) of the disagreed that they did not sign a confidentiality statement or form upon employment, while 9.8 of them did not know.

In the last 3 years (2011-2013) more than half 189(56.9%) of the respondents in the universities reported to have attended data security workshop or training facilitated by the institution, 119(35.9%) of them had not attended data security workshop or training facilitated by the institution in the period (2011-2013) while 24(7.3%) of them did not know.

185(55.7%) of the total respondents agreed that there existed a formal disciplinary process in place for employees who violate organizational security policies and procedures, 49(14.8%) of them disagreed that there existed a formal disciplinary process in place for employees who would have violated organizational security policies and procedures while 98(29.5%)of them did not know.

Slightly below half 146(44%) of the total respondents agreed that the information security policy was communicated to all employees on an ongoing basis. 90(27.1%) of them said the information security policy was not communicated to all employees on an ongoing basis, while a similar proportion of the respondents did not know whether the information security policy was communicated to all employees on an ongoing basis or not.

148(44.6%) of the respondents agreed that they were aware of spot checks or regular audits conducted by the ICT department to make sure staff access to electronic resources are not compromised by third party like hackers, almost a third at 105(31.6%) disagreed that they were aware of any spot checks or regular audits conducted by the ICT department to make sure staff access to electronic resources are not compromised by third party like hackers while 76(23.8%) of them did not know.

The results of the findings of confidentiality implies that it’s a 52 vs 48% scenario whereby compliance has small margin lead on no compliance (“No” & “Don’t Know”). This technically means confidentiality is very low and the institutions are at great risks in terms of confidentiality of information systems.

Security measures put in place in universities to enforce availability of information systems

The study sought to investigate security measures put in place in universities to enforce availability of information systems. The following table (table 7) provides a summary of Information systems availability questions with aggregated frequencies with the following columns/labels: "Yes", "No" & "Don't Know" that were asked to the respondents.

Table 7: Measures enforcing Availability

Information Systems Availability questions	**Yes Freq (%)**	**No Freq (%)**	**Don't Know Freq (%)**
Was is it made clear that you will be held accountable for your actions that made IT systems to fail or if you interfere with the system's operations?	190(58.3)	109(33.4)	27(8.3)
Do you have a step by step procedure on how to respond ICT security incidents like if you have reason to believe your system has been hacked?	152(47.1)	113(35.0)	58(18.0)
Do you have a procedure, to report security incidents through appropriate management person(s) as quickly as possible?	176(55.0)	85(26.6)	59(18.4)
Is the information security policy communicated to all employees on an ongoing basis?	144(45.0)	104(32.5)	72(22.5)
Are there procedures established to report any software malfunctions?	182(57.1)	58(18.2)	79(24.8)
Do you have a disaster recovery plan?	203(61.1)	31(9.3)	98(29.5)
Are backup media regularly tested to ensure that they could be restored within the time frame allotted in the operational procedure for recovery?	182(55.5)	116(35.4)	30(9.2)
Do you have an ICT continuity plan?	166(50.2)	48(14.5)	117(35.4)
Do you have specific employees or groups designated with maintaining and implementing the security policy?	212(67.3)	81(25.7)	22(7.0)
Average score (%)	55.1	25.6	19.2

From the table above more than half 194(58.3%) of the respondents agreed that it was made clear to them that they would be held accountable for any actions that made IT systems to fail or any interference with the system's operations. Slightly more than a third 111(33.4%) of the respondents disagreed that it was made clear to them that they would be held accountable for any actions that made IT systems to fail or any interference with the system's operations while 28(8.3%) of them did not know whether that it was made clear to them that they would be held accountable for any actions that made IT systems to fail or any interference with the system's operations.

156(47.1%) of the respondents agreed that there existed step by step procedure on how to respond to ICT security incidents like for instance if one had a reason to believe his or her system had been hacked. 116(35%) of them disagreed that there existed step by step procedure on how to respond to ICT security incidents like for instance if one had a reason to believe his or her system has been hacked, while 60(18%) of them did not know.

Slightly more than 166(50%) of the respondents agreed that they had procedures to report security incidents through appropriate management person(s) as quickly as possible, 88(26.6%) of them said that there were no procedures procedure to report security incidents through appropriate management person(s) as quickly as possible, while 61(18.4%) of them did not know whether there existed procedures to report security incidents through appropriate management person(s) as quickly as possible.

149(45%) of the total respondents agreed that the information security policy was communicated to all employees on an ongoing basis. 108(32.5%) of them said the information security policy was not communicated to all employees on an ongoing basis, while 75(22.5%) of the respondents did not know whether the information security policy was communicated to all employees on an ongoing basis or not.

190(57.1%) of the total respondents interviewed agreed that there were procedures established to report any software malfunctions, 60(18.2%) of them disagreed that there did exist procedures established to report any software malfunctions, while 82(24.8%) of them did not know whether there existed procedures established to report any software malfunctions or not.

Information availability dependents on the disaster recovery plan set out by the institution so that in cases of any eventuality they are able to revert back to normalcy. 202(61.1%) of the respondents in the Kisumu and Siaya Counties universities agreed that there existed disaster recovery plans, 99(29.5%) of them did not know whether there is disaster recovery plans or not while only 31(9.3%) of the respondents disagreed the existence of disaster recovery plans. More than half of the respondents confirmed that the backup media were regularly tested to ensure that they could be restored within the time frame allotted in the operational procedure for recovery, 118(35.4%) of them disagreed with that, while only 31(9.2%) did not know.

ICT need a continuity plan, this enables the environment to be maintained to current standards all the time. Amongst the campuses within the Kisumu and Siaya Counties half of the have ICT continuity plan, more than a third reported not be knowing whether there existed an ICT continuity plans or not. 223(67.3%) of the respondents agreed that there were specific employees or groups designated with maintaining and implementing the security policy, 85(25.7%) of them declined that there existed specific employees or groups designated with maintaining and implementing the security policy while only 23(7%) of them did not know.

Availability had a leading score of 55%. This implies that most systems in the institutions are likely to be available when needed. However, recommended minimum availability percentage of high availability systems is 95% which translates to 18 days of downtime in year. More needs to be done to realize high availability which in turn ensures reduced business risk in downtimes and lost opportunities due to downtimes.

CONCLUSION

Data analysis and interpretation revealed that majority of the learning institutions ranked very low on measures enforcing confidentiality of information systems. The greatest culprit here was password expiry with 38% compliance. This means that users used the same password for as long as they could remember; a very bad password policy. Other measures that ranked poorly include involvement of users in development of ICT policies and also that majority of users reported not having any audit spot checks. For compliance to ICT security policy to be in effect, the management needs to help facilitate audit spot checks, involvement of users in policy development and staff training in basic ICT security.

Data analysis and interpretation revealed that majority of institutions performed averagely in terms of availability. The worst performing measure was on the communication on ICT security policy on an ongoing basis and availability of step by step procedure on how to report to incidences. If ICT policy is not communicated across to all users, then clearly it becomes hard to enforce the policy. Most institutions have a policy gathering dust in some shelves whilst in contract it is supposed to be a living document.

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/