IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 08, Issue 3 (March. 2018), ||V2|| PP 73-81

Management Commitment as a Determinant of Information Security Awareness: A Case of Secondary Schools in Kenya.

OTIENO M.O.D[1]., LIYALA S[2]. and OGARA S[3].
Correspondions Autour: OTIENO M.O.D

ABSTRACT:- Securing information in any organization has become a key issue in the current digital age. Secondary schools, having adopted information systems to improve their effeiciency in service delivery are grappling with information security issues on the confidentiality, integrity and availability of information. These issues span around the people handling and using these information. School management plays a key role in information in terms of awareness of security policies, controls and risks by all school members. This study, therefore, sought to investigate the committment of schools management to information security as a determinant of information security awareness. The principals and system administrators in 21 secondary schools with running information systems were investigated in the survey using questionnaires. The collected data was analysed using statistical multiple linear regression and ANOVA. The study revealed that the management committment to information security in terms of policies, funding, compliance enforcement and awareness was low hence low level of information security awareness in the schools. The study recommends that schools' management be fully committed, aware and comply with information security practices to improve information security in the schools.

KEYWORDS: - awareness, determinants, information security, management.

Date of Submission: 26-02-2018 Date of acceptance: 13-03-2018

I. INTRODUCTION

Success in information security in any organization as stated in the ISO/IEC 17799 standard demands the commitment of its management. Every organization needs to protect its information assets and control how it flows within and without its boundaries by taking active steps to maintain the security of their information resources [1] For good information practices to be sustained they must be embedded in institutional culture [2] The critical nature of management commitment as a factor in any organization's information security is underscored by the senior management's responsibility for developing information security policies and the relevant controls, the provision of information security awareness programs, information classification, risk assessment, enforcing information security compliance and assignment of roles and responsibilities. The management's awareness of its own role as business leader enables it to have a grasp of information security to enable it to set policy objectives, take a leading role in security and define the critical assets that must be protected. It should understand the information security policy and controls, risks and their effects, information classification procedures, reporting procedures for information security breaches, security responsibilities and audits. The management's holistic commitment to information security is manifested, for example, by active participation in business continuity planning and being on top of information security management. Senior management commitment and support for information security is achieved through tying security risks to business objectives in order to understand the justification for security investment and provide the necessary resources for it. If the information security awareness of senior management is too low, user compliance will be low and confidence in the organization's information systems can vanish [3]. The top management commitment is critical to the design and effectiveness of information security program as it enables the alignment of enterprise governance with the information security governance framework [4] The management should have clear expectations about the information security program, how to evaluate the organization's risk posture and align information security objectives with the strategic goals of the organization.

Even though information security remains all users' responsibility in an organization, effective information security demonstrates commitment from top management that champions the importance of information security through a well-designed policy that ingrains information security as part of its culture. The ISO/IEC 27001 standard requires that organizations demonstrate leadership and commitment from top management by establishing an information security policy, defining and communicating information security responsibilities and roles and procedures for top management continual involvement in the evaluating information security program to ensure its effectiveness. The top management should oversight, support and direct the program through an information security policy that includes information security objectives, is appropriate to the organization and incorporates information security performance reporting. Making users to be aware of this policy is key to its success. The challenges of low level of management commitment is seen in information security practices such as risk assessment and analysis, security policies and controls implementation, awareness and training, security compliance, business continuity and disaster management.

Many human errors reported in the previous studies occur because of users' lack of awareness and understanding of information security issues [5].They result from failure by users to comply with an organization's information security policies and controls such as when users share passwords. Users need to be aware of information security policies together with the deployed information security controls to reduce the number of information security incidents in an organization [6]. Previous literature has argued that management is responsible in developing security awareness among users in the organization through conducting information security training and education program [7]. This improves employees' information security skills, encourages them to have good information security practices and as many authors on information security argue, achieve compliance to information security [8].

II. LITERATURE REVIEW

Even though information security is a basic requirement for business success, most top managements in many organizations often have only a superficial understanding of information security. This leads to decisions that do not auger well for the organization's information security. A senior management that understands and is committed to a successful information security program develops information security policy that reflects business needs tempered by known risks, informs users of their information security responsibilities as documented in security policy and procedures and establishes procedures for monitoring and reviewing the program [9]. The senior management must commit itself to and assume overall responsibility for information security and raise its own awareness level to enhance information security awareness among all employees.

Awareness according to NIST Special Publication 800-16 focuses attention on information security and is intended to allow individuals to recognize information security concerns and respond accordingly.

Skotnes, (2015) in her work "Management commitment and awareness creation – ICT safety and security in electric power supply network companies" found out that there was a strong relationship between management commitment to and the implementation of awareness creation and training measures for ICT safety and security in the companies [10]. High levels of management commitment were associated with high levels of awareness creation and training although her qualitative analysis revealed low levels of awareness despite investment in training by the power supply network companies.

Antilla (2006) in a paper, "senior executives commitment to information security, from motivation to responsibility" argues that despite the fact that information security is a basic requirement for business success, senior management often have only a superficial understanding of information security that leads them to make decisions that are not conducive to raising the organization's security level [11]. This shows the lack of senior management commitment to information security, a problem that is difficult to solve because many professionals think that it is not a good idea to "teach" their managers [12]. The low level of information security awareness of senior management of an organization might lead to low level of trust by stakeholders and is a proof of lack of management commitment. According to Allen (2013), survey results by PriceWaterhouse in 2013 confirmed the belief among IT security professionals that boards and senior executives were not adequately involved in key areas related to the governance of information security [13]. Of the pool of respondents, only 36% of them indicated that their board had direct involvement with oversight of information security although, most of those that reviewed privacy and security issues did not focus on activities that could help protect the organization from high risk areas such as reputational or financial losses resulting from breaches of personally identifiable information.

The senior management commitment is seen in its responsibility for compliance enforcement to information security requirements established for their users. They assign information security responsibilities, ensure the availability of resources and sufficiently trained personnel for implementing the information security program. They establish overall information security awareness and training strategy for all stakeholders and ensure that it is appropriate, timely and effectively deployed and reviewed [14]. They ensure that effective tracking and reporting mechanisms are in place to reduce errors and omissions due to lack of awareness and training. All this enables the organizations to protect the confidentiality, integrity and availability of their information assets in today's highly networked environment by ensuring that all people involved in using and managing information systems understand their roles and responsibilities related to the organizational mission, its information security policy, procedures, and practices and have adequate knowledge of the various management, operational and technical controls required and available to protect the information resources for which they are responsible. As cited in audit reports, periodicals, and conference presentations, it is generally understood that people are one of the weakest links in attempts to secure systems and networks. They are key to providing an adequate and appropriate level of security and need more attention and a robust awareness and training program to ensure that they understand how to properly use and protect the information resources entrusted to them. A good awareness and training program communicates security requirements across the enterprise leading to both management and user accountability [15]. Since awareness and training strategy is developed at the senior management level, the needs assessment to determine the strategy, the awareness and training plans, material and the methods of implementation throughout the organization is determined at this level. It must be designed with the organization mission in mind, support its business needs and be relevant to its culture. It should be focused on the organization's entire user population and the management should set the example for proper information security behavior. It should be deployed and aimed at all levels of the organization including senior managers and this calls for management commitment.

Users form the largest audience in any organization and are the single most important group of people who can help mitigate information threats and vulnerabilities [16]. Users may include employees, contractors, visitors, guests requiring information access. They are expected to understand and comply with security policies and procedures, know the rules of behavior for the systems and applications to which they have access, work with management to meet training needs and be aware of actions they can take to better protect information such as proper password usage, data backup, antivirus protection and reporting any security incidents or violations of security policy [17].

III. RESEARCH DESIGN AND METHODOLOGY

This study was carried out in secondary schools in Kisumu County in western Kenya region, a cosmopolitan region with secondary schools based in the city as well as rural settings. It has a total of 153 public secondary schools [18]. Purposive sampling was used to determine the 21 schools that had implemented ICTs by the time the study was undertaken and were using it in their daily teaching/learning and administrative activities as from 2011. (See appendix 1; Kisumu County Director of education office; 2015). These schools met the research criteria as they had experienced some information security challenges and the respondents were in a good position to answer questions on it appropriately. Purposive sampling was used to select the system administrators and school principals based on their functions in the schools.

The study adopted the research process onion with different layers starting from philosophies, approaches, strategies, choices, time horizons, techniques and procedures as described by Saunders, Lewis and Thornhill (2007) to guide it [19]. It adopted descriptive survey research design with positivism as the research position where the researcher used acceptable knowledge of existence of information security awareness programs in secondary schools to understand the effect of management commitment on them for effective information security.

The research followed a five-stage model deductive approach as suggested by Milyankova [20]; deducting a hypothesis from the theory, expressing the hypothesis in operational terms, testing the hypothesis, examining the outcome of the inquiry and modifying the theory in light of results. The time horizon for this research was cross sectional as this research was limited to a specific time frame. The researcher gathered the secondary data from journals, articles, magazines, websites and textbooks and collected primary data to answer the research questions and test the hypothesis. The use of questionnaires as the research instrument allowed the collected data to be standardized and to be easily compiled. The questionnaire was based on the ISO 27001; 2005 which lists the requirements for ISO 27002; 2005 code of practice for ISMS and used self-administered closed ended questions for prompt and honest responses, eliminating any bias that could have occurred in phrasing questions to different respondents. A peer review was done to gauge the suitability of the questions in relation to the research objectives (face and content validity) by exposing them to the university supervisors, peers in the faculty and other experts in IT sector. Based on their feedback, the necessary amendments were made to the questions. A pilot test was conducted in two secondary schools in Vihiga and Siaya Counties and the results used to modify and validate the questionnaire. In criterion-related validity**,** predictive validity was used to assess the ability to predict awareness and training from management commitment constructs by performing regression analysis between independent variables (management commitment) and corresponding responses on information security awareness and training as dependent variable. There were high correlations providing evidence for predictive validity, that these variables can correctly predict effective information security theoretically. This was backed by the regression coefficients that were found to be significant.

The researcher used the computation of Cronbach Coefficient Alpha to test the reliability of the questionnaires as recommended by Creswell and Clark [21] over the Kuder Richardson (KR) Formula or Spilt-half Reliability Coefficient. The Cronbach's alpha coefficient for the research instrument was found to be 0.895 and 0.946 for principals and system administrator responses respectively which was acceptable for reliability as illustrated in table 3.1

Table3.1: Cronbach’s reliability alpha for the study questionnaire.

	Cronbach's Alpha	Number of Items
Principals	.895	40
System administrators	.946	65

The questionnaires were dropped in to the respondents (secondary school system administrators and principals) and picked after a period of two to five days to allow enough time for response. Of the 21 system administrators and school principals, 20 administrators and 18 principals responded, a 95% and 86% response respectively. The responses were coded according to Lickert scale with five points (strongly agree, agree, not sure, disagree and strongly disagree). The collected data was then analyzed using frequencies, correlations and regression analysis to test the objectives. The collected data was analyzed using correlation and regression analysis tools in the Statistical Package for Social Scientist (SPSS) software version 20.0 and further validated using multiple linear regression analysis tests.

IV. RESULTS AND DISCUSSIONS

The study sought to find out the level of management commitment to information security in secondary schools in Kisumu County. The views of the respondents were collected on measures that were used to determine whether there was management commitment to information security in these schools and if it was effective. A total of 20 school system administrators and18 school principals submitted their responses. Both principals and system administrators were probed on their familiarity with information security, information handling in the schools, critical Information classified in the schools, development of policies, implementation and their interactions. All system administrators and 14 principals agreed to being familiar with information security. 45% of the system administrators and 34% of principals agreed that information handling in their schools was adequate as illustrated in the table 4.1.

Table 4.1: Responses in percentage of adequacy of information resources handling in the schools

Information handling in our school is adequate (%)	SD	D	NS	A	SA	Total
Principals	18	26	22	25	9	100
System administrators	40	15	0	35	10	100

The study listed the following as the critical information assets in secondary schools; student examination records, school fee records, staff and student personal records, equipment and physical facility records and financial transaction records which were affirmed by all the system administrators and principals as illustrated in the table 4.2.

Table 4.2: Responses in percentage of critical information resources in the schools

Information records considered in the study	Percentage agreeing to their criticality	
Respondent	System administrator	Principals
I consider examination records as critical for the school	100	100
I consider fee payment, arrears records as critical for the school	100	100
I consider staff records as critical for the school	100	100
I consider student records as critical for the school	95	100
I consider equipment and physical facilities records as critical for the school	90	100
I consider financial transaction records as critical for the school	100	100

1.1. Availability of Security Policy in Secondary Schools

The survey proceeded to find out if these secondary schools had ICT policy and information security policy in place. 60% of administrators reported that their schools had ICT security policy while 42% of the schools had a specific information security policy identified by users. 55% of users reported that the schools had an ICT use policy in place.

Policy development and implementation

The study looked at issues in policy development and implementation based on ISO 27001; 2005 policy requirements in tables 4.3 and 4.4 to the respondents. The results showed that policy development and implementation is not done in most schools and management commitment and co-ordination is low. Some principals were not even sure of this development.

Table 4.3: Policy development and implementation issues from system administrators

Policy Issue	Disagree (%)	Agree (%)
the policy is well documented and disseminated to all stakeholders e.g. by posters, on-screen notices, etc	60	40
the policy addresses purpose, scope, roles and responsibilities of stakeholders	40	45
the policy addresses management commitment and co-ordination for compliance	40	50

Table 4.4: Policy development and implementation issues from principals

Policy Issue	Disagree (%)	Agree (%)
the policy is well documented and disseminated to all stakeholders e.g. by posters, on-screen notices, etc	50	30
the policy addresses purpose, scope, roles and responsibilities of stakeholders	35	40
the policy addresses management commitment and co-ordination for compliance	50	30

The study also found out that key security controls were not implemented in many schools, a key indicator of management commitment. The results are shown in table 4.5 below.

Table 4.5: Distribution of security controls in secondary schools under the study from system administrators.

Security control	A	SA	TOTAL
we have identification and authentication measures such as ID cards, badges to control access to the information computer room.	3	3	20
there are measures for password management e.g. password length, expiry, characters, etc.	5	4	20
there are measures for recognizing and reporting information security incidents by users	4	2	20
users are educated/updated on security issues e.g. virus protection, password secrecy, unauthorized downloads and sites, etc	6	2	20
Anti-virus and malware is installed, updated and users forced to scan their devices.	7	3	20
there are backup and recovery procedures to ensure information is not lost	4	2	20
Information is encrypted before storing on backup removable media e.g. CDs, USBs, laptops.	2	1	20

1.2. Information security threats identified in the study

The study sought to find out if the respondents were aware and experienced information security threats based on the three key objectives of information security, CIA. The threats in the schools were identified as information loss, theft and destruction (55% agreed), modification (45%), leakage (55%) and denial of services (45%) from system administrators and 49%, 37%, 42% and 59% respectively from the principals. The results are shown in table 4.6.

Table 4.62: Information security threats identified in the study

Information threat Experienced	System administrators (%)					Principal's (%)				
	SA	A	NS	D	SD	SA	A	NS	D	SD
Information loss, theft and destruction	5	50	20	20	5	18	31	15	33	4
Information modification (unauthorized)	5	40	30	20	5	19	18	31	21	11
Information leaks	10	45	25	15	5	8	34	26	26	6
Denial of services	15	30	20	30	5	25	34	9	26	6

1.3. Effectiveness of information security awareness in schools

When the questions of whether the information security awareness was put to the respondents, the responses showed that only 35% of system administrators and 37% of principals agreed that their information systems security awareness program was effective as illustrated in the table 4.7.

Table 4.3: Responses on the effectiveness of information security awareness program in schools.

Respondent	In my view, information security is adequate				
	SD	D	NS	A	SA
System administrators	0%	35%	30%	30%	5%
Principals	18%	23%	21%	20%	17%

1.4. Effectiveness of awareness program based on security controls implemented in the study secondary schools

The study sought to find out if the security controls implemented in these schools indicated effective information security awareness. A regression test was run to test the correlations between the responses on security controls and effective information security awareness in the schools. From the correlations in table 4.17, it can be observed that most of the security controls observed by users have moderate to very weak correlations with effective security awareness in the study schools (r=.659 to r=.100) with correlation of backup to effective information security insignificant (p > 0.05). This indicates information security controls would significantly indicate information security awareness.

Table 4.4: Correlations between security controls and effective information security in schools (principals)

Security control observed/used.	Pearson's correlation, r	p- value (sig.)	Number of respondents
I scan all my devices before using them in the system	.387	.000	103
I use passwords	.326	.000	103
The passwords I use comply with the policy	.588	.000	103
I back up my documents according to the policy	.100	.156	103

This was further confirmed by results of the regression model summarized in table 4.18 for principals' responses which showed that 54% of effective information security responses are explained by the security identified security controls at 95% confidence interval (p<0.05) and confirmed in the ANOVA (see table 4.18) where, the F-value is significant, F (9, 93)= 12.166, p<0.05, indicating that there is significant relationship between the security controls implemented in the schools and the effective information security.

Table4.5: Regression Model for relationship between security controls and effective information awareness from principals

<table>
<tr><td rowspan="2">Model</td><td rowspan="2">R</td><td rowspan="2">R Square</td><td rowspan="2">Std. Error of the Estimate</td><td colspan="2">Change Statistics</td><td colspan="2" rowspan="2">Durbin-Watson</td></tr>
<tr><td>R Square Change</td><td>Sig. F Change</td></tr>
<tr><td>1</td><td>.735[a]</td><td>.541</td><td>.983</td><td>.541</td><td>.000</td><td colspan="2">1.855</td></tr>
<tr><td colspan="8">ANOVA</td></tr>
<tr><td colspan="3">Model</td><td>Sum of Squares</td><td>Df</td><td>Mean Square</td><td>F</td><td>Sig.</td></tr>
<tr><td rowspan="3">1</td><td colspan="2">Regression</td><td>105.793</td><td>9</td><td>11.755</td><td>12.166</td><td>.000[b]</td></tr>
<tr><td colspan="2">Residual</td><td>89.858</td><td>93</td><td>.966</td><td></td><td></td></tr>
<tr><td colspan="2">Total</td><td>195.650</td><td>102</td><td></td><td></td><td></td></tr>
</table>

Most of the security controls observed by system administrators had moderate correlations with effective security in the study schools which are significant (r= .798 to r= .506) and (p<.05) as shown in table 4.19. This indicated the strong relationship between management commitment and information security awareness in the schools.

Table 4.6: Correlations between security controls and information security awareness in schools (system administrators)

Security controls from system administrators' Responses.	Pearson's correlation, r	p-value	Number of respondents
there are measures to verify individual access authorizations before granting access	.608	.002	20
there are measures for recognizing and reporting information security incidents by user	.597	.003	20
users are educated/updated on security issues e.g. virus protection, password secrecy, unauthorized downloads and sites, etc.	.798	.000	20

anti-virus and malware is installed, updated and users forced to scan their devices with anti-virus	.653	.001	20
there are backup and recovery procedures to ensure information is not lost	.781	.000	20
information is encrypted before storing on backup removable media e.g. CDs, USBs, laptops, etc.	.692	.000	20

The model summary in table 4.20 shows that 84% of all responses on effective information security awareness by system administrators can be explained by the responses on security controls at 95% confidence level ($p < 0.05$) indicating that compliance to the security controls in the schools indicated the effectiveness of information security awareness program. This is confirmed in the ANOVA table 4.22 where the F-value is low but significant, F (13, 6) = 3.139, $p<0.05$.

Table 4.7: Regression Model on relationship between security controls and information security awareness from system administrator response

Model	R	R Square	Std. Error of the Estimate	Change Statistics		Durbin-Watson
				R Square Change	Sig. F Change	
1	.918	.842	.791	.842	.000	2.132
ANOVA						
Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	14.777	13	1.137	3.139	.004
	Residual	2.173	6	.362		
	Total	16.950	19			

Table4.8: Correlations between security controls and information security awareness in schools (principals)

Security controls from system administrators' Responses.	Pearson's correlation, r	p-value	Number of respondents
there are measures to verify individual access authorizations before granting access	.599	.002	18
there are measures for recognizing and reporting information security incidents by user	.624	.002	18
users are educated/updated on security issues e.g. virus protection, password secrecy, unauthorized downloads and sites, etc.	.607	.003	20
anti-virus and malware is installed, updated and users forced to scan their devices with anti-virus	.573	.002	18
there are backup and recovery procedures to ensure information is not lost	.521	.003	18
information is encrypted before storing on backup removable media e.g. CDs, USBs, laptops, etc.	.673	.000	18

Table 4.9: Regression Model for relationship between security controls and information security awareness from principals**.**

Model	R	R Square	Std. Error of the Estimate	Change Statistics		Durbin-Watson
				R Square Change	Sig. F Change	
1	.735[a]	.541	.983	.541	.000	1.855
ANOVA						
Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	105.793	9	11.755	12.166	.000[b]
	Residual	89.858	93	.966		
	Total	195.650	102			

V. CONCLUSION

The main objective of this study was to determine the effectiveness of management commitment on information security awareness in secondary schools in Kenya. Based on the data collected, it was found out that management commitment is a key determinant to effective information security awareness in these schools. Data analysed indicated that there was strong relationship between management commitment and information security awareness, r= 0.918 and r^2= 0.842 for system administrators and r = 0.735 and r^2 = 0.541 for school principals. The identified challenges included school principal's lack of information security awareness, delegation of information security to system administrators, lack of awareness and security policies.

REFERENCES

[1] Doherty, N.F. (2011). Information Security Policies in Large Organisations: Developing a Conceptual Framework to Explore their Impact; the Business School, Loughborough University, Loughborough, UK; http://dx.doi.org/10.1016/j.ijinfomgt.2010.06.001. accessed on 11/05/2015.

[2] Gaible, E. (2008). Survey of ICT and Education in the Caribbean: A summary report, Based on 16 Country Surveys. Washington, DC: info Dev / World Bank. Available at hppt://www.infodev.org/en/Publication.441.html; downloaded on 2/04/2015.

[3] Albrechtsen, E. (2006), "A qualitative study of users' view on information security", Computers & Security , Vol. 26 No. 4 [accessed on 10 Nov 2017]

[4] Imszennik Jay; 2016; ISO 27001: Role of Top Management and Its Importance; https://www.schellman.com/blog/2016/01/iso-27001-role-of-top-management/ Jan 15, 2016.

[5] M. Siponen, et al., 2010, "Compliance with Information Security Policies: An Empirical Investigation," Computer, vol. 43, pp. 64-71.

[6] Vance A., et al. 2012. "Motivating IS security compliance: Insights from Habit and Protection Motivation Theory," Information & Management, vol. 49, pp. 190-198, 2012

[7] Humaidi, N., & Balakrishnan, V. 2015. The Moderating effect of working experience on health information system security policies compliance behavior. Malaysian Journal of Computer Science, 28(2), 70-92.

[8] Wright Craig, S., 2005. Implementing an Information Security Management System (ISMS) Training process. G7799 Practical Assignment Version 1.1 SANS Institute 2000 – 2005. www.SANS.org.

[9] Skotnes, Ruth Østgaard , (2015) "Management commitment and awareness creation – ICT safety and security in electric power supply network companies", Information & Computer Security, Vol. 23 Issue: 3, pp.302-316, https://doi.org/10.1108/ICS-02-2014-0017

[10] Anttila Juhani. 2006. Senior Executives Commitment To Information Security - From Motivation To Responsibility; Venture Knowledgist Quality Integration; Helsinki, Finland; Www.Qualityintegration.Biz

[11] Besnard, D. and Arief, B. (2004), "Computer security impaired by legitimate users", Computers & Security , Vol. 23 No. 3, pp. 253-264. [accessed on 10 Nov. 2017]

[12] Allen Julia H. 2013; Security Is Not Just a Technical Issue Published: May 13, 2013 Carnegie Mellon University. https://www.us-cert.gov/bsi/articles/best-practices/governance-and-management/security-is-not-just-a-technical-issue

[13] Greene, Sari., 2014. Security Program and Policies: Principles and Practices, 2nd Edition. Pearson IT Certification. [accessed on 12 Dec 2017]

[14] Xiao, Z., Kathiresshan, N., and Xiao, Y. 2016. A survey of accountability in computer networks and distributed systems. Security Comm. Networks, 9: 290–315. doi: 10.1002/sec.574.

[15] Rossi, Ben., 2014.Educating the end user and eliminating the biggest security risk 'The most effective way the CIO can deliver practical and memorable education is to make it real.' Dell Secure Works. 19 June 2014. [Accessed on 12 Dec 2017]

[16] Rader, Emilee. & Wash, Rick., 2015. Identifying patterns in informal sources of security information. Journal of Cybersecurity, Volume 1, Issue 1, 1 September 2015, Pages 121–144, https://doi.org/10.1093/cybsec/tyv008

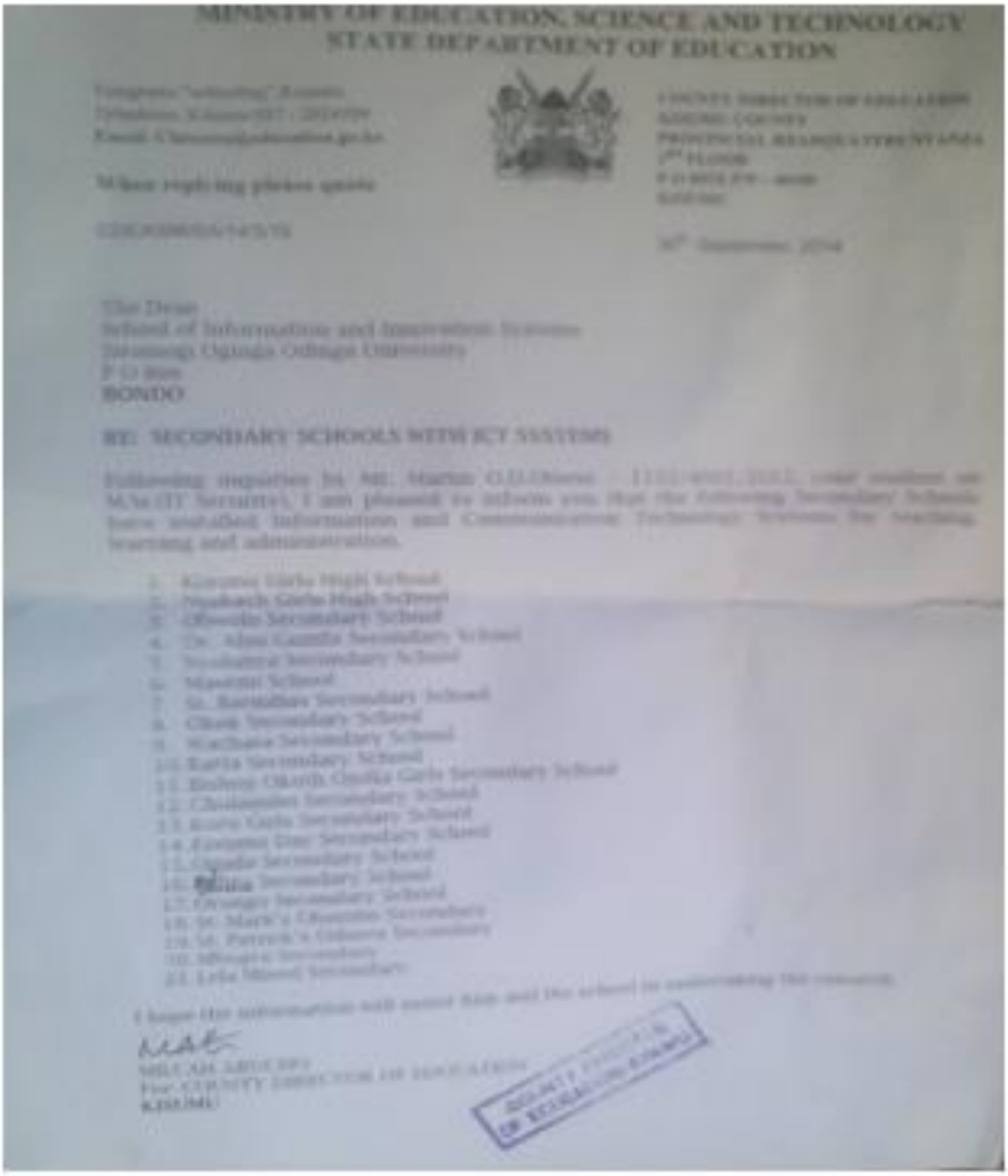
[17] softkenya.com., 2010. List of Kenyan Secondary Schools. www.softkenya.com. [Accessed on 01 Oct 2017]

[18] Saunders, M., Lewis, P. and Thornhill, A. (2007) Research Methods for Business Students. 4th Edition, Financial Times Prentice Hall, Edinburgh Gate, Harlow.

[19] Milyankova, R. (n.d.). Lecture 7 Choosing Research Strategy and Approach. [online] Iuc-edu.eu. Available at: http://www.iuc-edu.eu/group/sem1_L2/PDEVR2010/_7_Choosing%20strategy_method.ppt [Accessed 01 Oct. 2017].

[20] Cresswell, J. W., & Clark, V. L. P. (2011). Designing and conducting mixed methods research. Los Angeles: Sage.

Appendix 1: List of schools with running information systems in Kisumu county that were active from 2010



MINISTRY OF EDUCATION, SCIENCE AND TECHNOLOGY
STATE DEPARTMENT OF EDUCATION

Telegrams "[illegible]" Kisumu
Telephone: Kisumu 057 - [illegible]
Email: [illegible]@education.go.ke

When replying please quote

CDE/KSM/[illegible]

COUNTY DIRECTOR OF EDUCATION
KISUMU COUNTY
PROVINCIAL HEADQUARTERS NYANZA
[illegible] FLOOR
P.O BOX [illegible]
KISUMU

[illegible] September, 2014

The Dean
School of Information and Innovation Systems
Jaramogi Oginga Odinga University
P O Box
BONDO

RE: SECONDARY SCHOOLS WITH ICT SYSTEMS

Following inquiries by Mr. Martin O.D.Otieno – [illegible], your student on M.Sc (IT Security), I am pleased to inform you that the following Secondary Schools have installed Information and Communication Technology Systems for teaching, learning and administration.

1. Kisumu Girls High School
2. Nyakach Girls High School
3. [illegible] Secondary School
4. Dr. [illegible] Secondary School
5. [illegible] Secondary School
6. Maseno School
7. St. Barnabas Secondary School
8. [illegible] Secondary School
9. [illegible] Secondary School
10. [illegible] Secondary School
11. Bishop Okoth Ojolla Girls Secondary School
12. Chulaimbo Secondary School
13. Koru Girls Secondary School
14. Kisumu Day Secondary School
15. Ogada Secondary School
16. [illegible] Secondary School
17. [illegible] Secondary School
18. St. Mark's [illegible] Secondary
19. St. Patrick's [illegible] Secondary
20. [illegible] Secondary
21. Lela Mixed Secondary

I hope this information will assist him and the school in undertaking the research.

MILCAH [illegible]
For: COUNTY DIRECTOR OF EDUCATION
KISUMU

COUNTY DIRECTOR OF EDUCATION KISUMU

OTIENO M.O.D " Management Commitment as a Determinant of Information Security Awareness: A Case of Secondary Schools in Kenya..” IOSR Journal of Engineering (IOSRJEN), vol. 8, no. 3, 2018, pp. 73-81.