International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 7 Issue 5, May 2020

ISSN: 2394-4404

An Information Security Awareness Framework For Secondary School Teachers In Kenya

Gloria Awuor Odiaga

Silvance Abeka

Samuel Liyala

Department of Computer Science and Software Engineering,
Jaramogi Oginga Odinga University of Science and Technology, Kenya

Abstract: ***Over the last decade, secondary schools have increased ICT usage in teaching and learning. The technological devices mostly belong to students and staff hence advancing the BYOD culture that makes the ability of the school to impose information security measures problematic especially with the growing number of cyber-attacks. This creates backdoor access to sensitive and personally identifiable information on students, staff and parents which if infiltrated by cyber criminals can be sold for profit or exchanged for large ransom payments. Unfortunately, secondary school teachers are yet to have comprehensive awareness of information security practices. The purpose of this paper is to provide a validated framework for information security awareness among secondary school teachers. A total of 172 respondents from 86 Kenyan secondary schools participated in this survey. The results show that the teachers lacked access to information security education and had little or no knowledge of basic information security awareness practices, roles, threats, risks and attacks, hence there is a need for a framework for information security awareness based on Endsley's Theory of Situational Awareness. This study provides useful insights for policy and practice in the education sector on improving information security awareness of secondary school teachers.***

Keywords: Information Security Awareness, Endsley's Theory of Situational Awareness, Cyber-attacks, Framework, Threats, Risks, BYOD.

I. INTRODUCTION

Globally, ICT is the backbone of all sectors and this increased dependence on information systems has resulted in a corresponding increase in information security abuses. Teachers need to adjust with the new paradigm shift due to the demand of ICT in all teaching and learning levels (Mbogo, Onunga & Kirathi, 2014). The importance of ICT in teaching and learning cannot be understated (Al-Janabi & Al-Shourbaji, 2016; Chan & Mubarak, 2012). The lack of information security awareness and knowledge can be attributed to numerous information security risks present in organizations and institutions (Ahlan, Lubis & Lubis, 2015). There is need to be aware of such risks, guide people against committing risky acts as well as adopt countermeasures and policies that can help promote information security awareness (Aloul, 2012).

The education sector lags in adoption of information security awareness programs; hence there is increase in information security breaches (Rajewski, 2013). These information security breaches have led to actual financial losses for institutions, negative publicity, reduced academic or organizational viability and competitive disadvantage (Aloul, 2012). Lack of information security awareness is not limited to given countries, but it is a global issue. In the United States, most schools are at a high risk of cyber-attacks and a high number of students are involved in information security breaching (Gurney, 2014). The United Kingdom (UK) has also had information security breaches doubled within the last decade (Ahlan et al., 2015). The United Kingdom has

established initiatives such as cyber security lessons for students (Gurney, 2014). This also increases the information security awareness of their teachers to manage the risk of information security breaches. Internationally, emphasis on information security awareness is a key strategy for organizations to protect their reputation as well as minimize the financial losses associated with information security breaches (Farooq, Isoaho & Virtanen, 2015). A study by Al-Janabi and Al-Shourbaji (2016) reveals that an all-inclusive information security awareness and adoption of training programs in institutions would improve the state of information security awareness.

Educational institutions are the most vulnerable when it comes to high crime rates, hackers, information loss, cyber bullying and human trafficking (Gurney, 2014). The executors of these crimes have several avenues to gather information about their victims, hence; learners and teaching staff must be made aware of the benefits of information security awareness (Gurney, 2014; Okuku, 2015). In Kenya's education sector, information security is a primary problem, especially in secondary schools and universities due to increased examination cheating, hacking of administrative information, duplication of others' work amongst others; experts reveal that improving information security awareness in schools, especially among teachers, may help reduce information security breaches (Oduor, 2015; Ojwang, 2012). Information security awareness has become precedence for most schools and institutions in Kenya (Oduor, 2015). Secondary schools can develop special programs to teach information security skills to students in order to augment the information security awareness status amongst teachers as they have to train and gain knowledge on the same before passing it on to students, hence there is need to address key aspects that impact on information security education (Mbogo et al., 2014).

In light of the above, this study provides a framework for information security awareness among secondary school teachers. The framework based on Endsley's theory of Situational Awareness focuses on the perception and comprehension of the factors in the environment, and the forecast of their future status.

II. LITERATURE REVIEW

A. STATUS OF INFORMATION SECURITY AWARENESS

According to Bulgurcu and Benbasat (2010), the attitude of employees is affected by their status of information security awareness. As such, putting emphasis on information security awareness can positively impact on employees attitudes, which in turn encourage their compliance. The study suggested that information security awareness must be taken into consideration when devising any risk mitigation strategies or frameworks in the organizational context. (Okuku, Renaud & Valeriano, 2015). User information security awareness influences their views and contribution towards security policies and is therefore a major aspect in ensuring information security in an organization (Farooq et al., 2015). The research performed by Doherty, Anastasakis and Fulford (2009) explored the structure of information security frameworks for Universities based in the United Kingdom. The study contributed to literature on how the university management fosters a comprehensible approach to information security and risk management. While the study filled the gap in the literature by analytically assessing the content of information security frameworks, it did not directly explore information security awareness as a primary aspect of the implementation of these policies.

Similarly, the study by Chan and Mubarak (2012) explored the significance of information security awareness in the higher education sector within the Australian organizations' context. The findings of their study showed that the status of information security awareness of the employees were low since they lacked both in awareness of the organization's information security frameworks and knowledge of concepts. The study indicated that employees confirmed to have previously participated in password sharing, which is a direct violation of security of information. Chan and Mubarak (2012) suggest that such behaviors are as a result of lack of framework enforcement and promotion.

The study by Ojwang (2012) identified that e-learning readiness and information security awareness remains a challenge in Kenyan educational institutions which do not have adequate information security awareness programs in place to offset the worrying status of information security awareness; thus compliance is low. Therefore, it is imperative to adapt information security awareness programs to nurture a culture of compliance that will eventually enhance employees or staff compliance to information security. Kenyan schools are marred with several information security breaches including exams cheating, loss of private information and other cyber security crimes (Oduor, 2015). To address these challenges, Oduor (2015) recommended the need for information security awareness in educational institutions. Nonetheless, he recognized that secondary schools can develop specialized programs to teach skills in information security to students while widening the scope of knowledge for the teachers. As a result, the status of information security awareness will significantly increase amongst the staff members. Kimwele, Mwangi and Kimani (2011) also explored the information security framework for Kenya's small and medium enterprises (SMEs). Their study attributes the lack of information security awareness and knowledge to the numerous information security risks present in the Kenyan SMEs.

School systems in Kenya are now enabled to store and access information on students, staff and operational issues with ease (Oduor, 2015). The perceptions and experiences of teachers and administrators play an important role in the use of computers in Kenyan classrooms (Mbogo et al., 2014). Hackers and fraudsters emerged as the major security violators (Mbogo et al., 2014); this confirms the possibility of information security breaches to vulnerable populations such as secondary school teachers. When teachers get to use technology, they constantly expose themselves to electronic and physical threats such as organized crime for the purpose of content defalcation, database disruption, information flow monitoring, and violation of intellectual property rights (Okewa, 2011).

From these studies, it can be deduced that employee information security awareness is internationally perceived as an important contributing aspect in any successful organizational information security strategies. Nevertheless, there is a gap in literature since very little has been done in the Kenyan context with regards to information security awareness, thus prompting the need for this study. Also, the studies do not explicitly discuss the implications of user information security awareness. The studies only identify information security awareness as a key factor when assessing an organization's risk management and user compliance. Examining the need for information security awareness is considered to be the preliminary step in achieving information security readiness (Oduor, 2015). The following step would inherently be, to assess the current state of information security awareness, investigate the factors that affect information security awareness then, to develop an information security awareness framework for secondary school teachers.

B. FACTORS AFFECTING INFORMATION SECURITY AWARENESS AMONG SECONDARY SCHOOL TEACHERS

ICT in African countries continues to lag in implementation compared to Western and Asian countries, and this continues to widen the digital and knowledge divides; Kiptalam and Rodriguez (2010) observed that one of the major challenges that face most African countries is access to ICT facilities with a ratio of one computer to 150 students while that of developed countries is at a ratio of 1:15 students. The cost of adopting proper ICT infrastructure, including acquiring hardware and software, setting up telecommunication networks, and the maintenance and repair of facilities is often prohibitive for developing nations (Okuku et al., 2015). Computers are still very expensive for internet connectivity to run effectively; yet most school management boards put more emphasis on health care, food and other amenities when making budget plans as they do not see the need to purchase and subsequently install computers in their schools as a priority (Okewa, 2011).

Good governance and management is required in ensuring there is no breach of information security. Mbogo *et al.*, (2014) noted that many developing nations lack ICT policy, have poor ICT management, and corruption has led to ineffective implementation, adoption of different systems and standards, duplication of effort, and waste of technology resources. Many times, efforts are often uncoordinated and initiatives are in competition with each other rather than complementing each other; this leaves the security of the system unsupervised or as a nobody's business (Gurney, 2014). There are also instances where many unsustainable ICT programs exist, where schools have computers that do not work or are misused (Mbogo et al., 2014).

There is still a strong perception, especially by the older generation, that ICT require highly skilled personnel to operate them; while this may not be the case, some school administrators have not taken their time to familiarize themselves with the technology and security information that comes with it (Oduor, 2015; Okewa, 2011). Some teachers fear the infection of viruses to their computers leading to data loss; while this may be true to some extent, proper education on the safe use of computers can help alleviate some of these fears (Okewa, 2011). Limited computer knowledge, which is precipitated by the reluctance or inability of schools to introduce ICT, often results in limited use of resources and limited awareness of information security (Gurney, 2014). Inadequate educational software in the schools leaves the responsibility to the teachers, and this is seen as an extra expense that the teachers are not ready to cater for on behalf of the schools (Ojwang, 2012).

C. INFORMATION SECURITY AWARENESS FRAMEWORK

The major emphasis on this study was information security awareness, therefore it is imperative to examine the theories of how human beings acquire and establish awareness. Most of the theories stem from cognitive theories and human factor paradigms. Some scholars such as Curts and Campbell (2001) stated that the observe, orient, decide and act (OODA) loop and cognitive hierarchy can be relevant in comprehending how human beings gain knowledge and then act. Also, the Shewhart cycle, commonly known as the Deming cycle of Plan-Do-Check-Act (PDCA) theory explains a recurrent approach to performing tasks (Moen & Norman, 2006). Another new framework is Situational Awareness, which was used for this study.

D. ENDSLEY'S THEORY OF SITUATIONAL AWARENESS

Endsley (1995), defined Situational Awareness as perception of factors existing in the environment, their meanings, proper comprehension, and the forecast of their future status. Situational Awareness explores how humans are aware of the cues or information within their environment, how they determine their next course of action and the consequences of their actions (Endsley, 2016). Therefore, Situational Awareness offers a framework that can be used for information security awareness since many information security breaches are attributed to human errors (Endsley, 2016); for instance, people have knowledge of computer viruses yet they still readily open links and attachments due to the lack of information security awareness of the risks related to their actions.

The concept of Situational Awareness has gained considerable recognition and has been used in several researches since the early days. As stated by Stanton, Chambers and Piggot (2001), the idea of situational awareness was recognized during the First World War by Oswald Boelcke who identified the significance of acquiring awareness of the enemy before the latter acquired similar awareness, and established mechanisms for achieving this.

The concept of separation between the human operators' comprehension of system status and actual system is at the heart of the definition of situational awareness (Endsley, 2016). Stanton et al., (2001) noted that people can obtain adequate awareness of the system status only if they track the progress of events as they unfold. They contend that incidents

ISSN: 2394-4404

happen as a result of the proliferation of disturbances over time. These problems worsened if human controllers do not adapt to the new events. This can result in disentanglement of system state and the human operators' comprehension of the system where human situational awareness separates from the actual system state. The significance of situational awareness in ensuring information security cannot be overstated for the purpose of this study.

Therefore, by assessing the status of information security awareness and the factors that affect information security awareness of the teachers in secondary schools, this study develops a framework for information security awareness based on Endsley's theory of Situational Awareness.

E. CONCEPTUAL FRAMEWORK

In this study, information security awareness is the dependent variable while the two main independent variables are status of information security awareness and factors affecting information security awareness. The status of information security awareness was informed by access to information security education, basic information security practices and basic knowledge of information security roles, threats, risks and attacks while the factors that affect information security awareness include ICT infrastructure, resources and personnel, technical knowledge/skills in ICT, qualification level, management support and information security policy and risk management. The framework recognizes three levels based on Endsley's theory of situational awareness crucial for the mitigation of information security risks in secondary schools. Level 1 is the perception of key elements that give a mental picture of the status of information security awareness of the teachers while level 2 is the comprehension of the elements in Level 1 to define the situation operationally by understanding the factors that affect information security awareness. Level 3 is the projection of the future status; the ability to project the events that might happen based on the analysis and extrapolation of the information in level 1 and the results of the actions in level 2 forward in time to ensure information security awareness of the secondary school teachers.

In the presence of an overarching government policy on information security awareness, schools may be more aware and concerned about information security. Information security awareness is important and the Government and school managements should provide more opportunities for training initiatives. This is a critical factor because institutions with information security awareness programs and training initiatives are more likely to have members of staff that are cautious about information security, hence are likely to have greater information security awareness. Figure 1 below summarizes the conceptual framework of the study. The relationship between the variables of the study is shown. Any change in the independent variables will affect either positively or negatively, the extent of information security awareness among secondary school teachers.

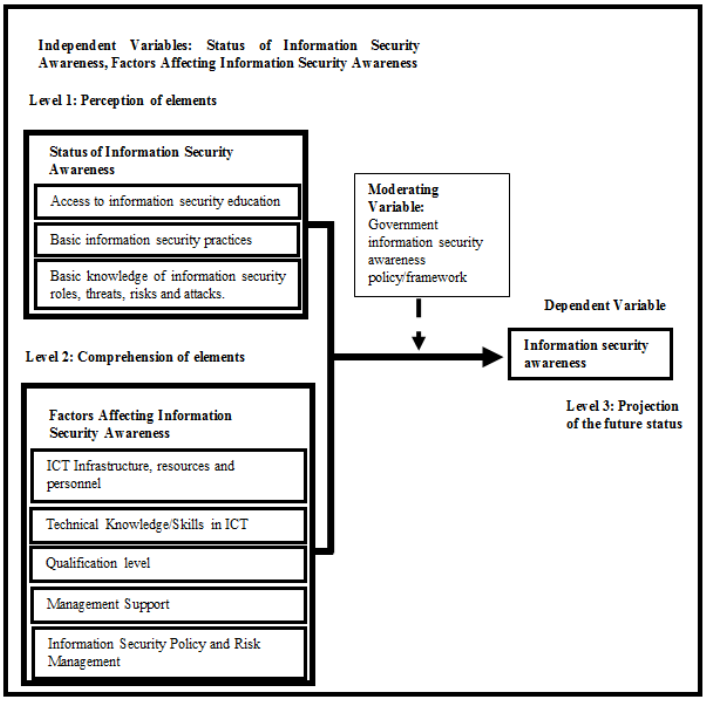

Figure 1: Conceptual Framework

III. RESEARCH METHODOLOGY

The study took the form of a descriptive survey with quantitative methods in order to investigate and provide an understanding of information security awareness among teachers. The target population was principals and teachers in the public secondary schools in Kisumu County. There are 570 secondary school teachers who have integrated the use of ICT in teaching and learning in 110 secondary schools in Kisumu County (Kenya Open Data Portal, 2014). Therefore, 570 teachers and 110 principals make a total study population of 680 individuals.

The sample size was determined using Yamane's formula (Yamane, 1967): n = N / [1+N (e) ^2] where: n = sample size, N = population size, e = sampling error (0 .05) therefore: n= 110/[1+110(0.05)^2]=86 schools. The sample size used was 86 schools which were selected using a multistage sampling approach which involves recruiting the sample in stages (Bryman, 2008). Smaller and smaller samples were recruited in each stage. The use of multistage sampling in this study was informed by the characteristics of the target population. Four levels were used to classify public secondary schools in the study area; sub-county level; school jurisdiction as national, extra county, county and district schools; composition as boys-only, girls-only, or mixed schools, and operation status as day, boarding, or day and boarding schools. It was crucial for all these categories to be represented in the sample. Simple random sampling was used to select schools from each cluster.

Purposive sampling was used to identify six individuals per school (one principal and one head of department), giving a total of 172 respondents. Purposive sampling is a non-probability sampling technique where subjects are selected based on the objective of the study and, most importantly, the capacity of the participants to provide the required information

(Bryman, 2008). To obtain useful information about information security awareness, it was important to use participants in a position to do so or with a better understanding of the topic. In this regard, principals and head of departments who occupy more authoritative positions were deemed appropriate respondents for the study. The respondents were required to provide information about information security awareness and factors that affect their awareness of information security.

Given that the study was a descriptive survey research, a questionnaire was used as the instrument for data collection. This tool was chosen because of its ability to collect a large amount of data from a large population in a short period. It also ensures that all subjects receive the same questions. In addition, the researcher is able to keep a record of the responses for not only data compilation for the current study, but also for future referrals. The aim of the study was to describe information security awareness among secondary school teachers in the study area and develop a validated framework for governance, hence the appropriateness of a researcher-designed questionnaire.

The reliability test measures the extent to which results produced by the instrument are consistent. Internal consistency reliability is a measure of how well the items on a test measure the same construct or idea. The Cronbach Alpha co-efficient was calculated on the piloted questionnaire to measure the internal consistency of items in the questionnaire. A higher value means that the instrument is more reliable, and vice versa (Mohsen & Dennick, 2011). Typically, a value of 0.75 and above indicates sufficient instrument reliability. Using the Statistical Package for Social Sciences (SPSS version 17), the instrument returned a value of 0.88 which is within the expected range.

The validity test answers the question of whether an instrument measures what it is intended to measure (Bryman, 2008). Face and content validity of the instrument was ascertained by giving copies of the questionnaire to the research supervisors so as to examine closely and ensure face and content validity. Their comments and suggestions were used to revise the questionnaires before making the final one. The content validity refers to the representativeness of the item content domain or the manner in which the questionnaire and its items are built to ensure the reasonableness of the claims of content validity (Bryman, 2008).

IV. RESULTS

Prior to the actual analysis, the data was first cleaned and coded then keyed into the analysis software. Descriptive statistics were used to analyze and present the results; frequencies and averages (mainly depicted as numerals or percentages) as well as tables were used to describe the status of information security awareness amongst the participants as well as the factors that affect their awareness. Inferential statistics in form of mathematical regression analysis was also used in developing the mathematical model used in validating the developed framework for information security awareness among secondary school teachers.

Questionnaires were sent to a total of 172 respondents. Of these, 169 were returned, translating to a response rate of 98%. Nonetheless, of the returned questionnaires only 122 were usable (72%). The rejected questionnaires were characterized by numerous unanswered or incomplete responses, making them unusable. All the same, 72% was considered an acceptable response rate as the study focused on respondents who might have been busy with administrative tasks, teaching work, or other businesses. Table 1 below summarizes the response rate of questionnaires sent to respondents.

Sent	Returned	Discarded	Valid	Final response rate (%)
172	169	47	122	72

Table 1: Response Rate

64% of the respondents were male, 54% were principals and 68% had more than five years of teaching experience. Table 2 below summarizes the characteristics of the respondents.

Characteristics	% of Respondents
Gender	
Male	64%
Female	36%
Designation	
Principal	54%
Head of Department	46%
Teaching Experience	
0-5 years	32%
Over 5 years	68%

Table 2: Characteristics of Respondents

STATUS OF INFORMATION SECURITY AWARENESS

a. ACCESS TO INFORMATION SECURITY EDUCATION

71% of the respondents indicated that they had not received any information security training and of the 29% that indicated receipt of information security training, 83% indicated that they had received the training at the university or college; none had received the training at their place of work or in seminars.

b. INFORMATION SECURITY PRACTICES

Only 34% indicated putting a password protected screensaver to secure their computers from unauthorized access as opposed to turning off the monitor or computer. 65% of the respondents were likely to open email attachments as long as they knew the sender of an email. Also, 65% of the respondents had shared login details and passwords with their colleagues. Further, 70% indicated that their name or school name would be a strong password while 68% indicated that documents with personal information at their workplace were not handled in any special manner.

c. KNOWLEDGE OF BASIC INFORMATION SECURITY ROLES, THREATS, RISKS AND ATTACKS

40% of the respondents did not find spam mail annoying, 47% thought the internet is safe, 69% had no problem with forwarding chain emails or messages and 58% were convinced that the internet cannot be used to hurt others. Further, 47% of the respondents were either indifferent or saw no problem with using a computer without anti-virus software. Also, 51% were convinced that personal data cannot be used to make money and 56% would wish to view personal data of others if it could be viewed freely. Also, 55% of the respondents were convinced that security measures are an organizational responsibility, not an individual responsibility. The responses are summarized in Table 3 below.

Question	Disagree strongly	Disagree	Difficult to say	Agree	Agree Strongly
Can personal data (address, name, email address, etc.) be used to make money?	33%	18%	22%	15%	12%
If the personal data (address, name, email address, etc.) of others could be viewed freely, would you wish to see it?	25%	7%	12%	45%	11%
Is there a problem in using a computer that does not have anti-virus software installed?	23%	12%	18%	28%	19%
Is there a problem with forwarding a chain email or message to a friend or colleague?	53%	16%	15%	11%	5%
Do you find spam or junk mail annoying?	16%	24%	23%	18%	19%
Is there a problem with web browsing history being monitored as a security measure?	15%	13%	20%	45%	7%
Do you think that security measures are up to the school and not an individual employee?	15%	11%	19%	33%	22%
Do you think internet is safe?	12%	13%	28%	31%	16%
Can people be hurt through internet?	44%	14%	20%	15%	7%
Do you think that anything on your work computer is of interest or value to others?	21%	7%	30%	36%	16%

Table 3: Knowledge of basic information security roles, threats, risks and attacks

FACTORS AFFECTING INFORMATION SECURITY AWARENESS

a. ICT INFRASTRUCTURE, RESOURCES AND PERSONNEL

74% of the respondents indicated that the number of computers in their school was inadequate. 47% felt that the cost of internet connection was too high for their school to afford and only 32% reported that their schools had ICT technicians, with 65% agreeing that the lack of ICT teachers or experts was a barrier to the ICT integration in their schools. Also, two thirds of the respondents said they shared a computer with colleagues, however, only 15% indicated that each user had a separate log in account.

b. TECHNICAL KNOWLEDGE/SKILLS IN ICT/QUALIFICATION LEVEL

45% of the respondents specified that their schools provided for access to the internet e.g. through modems, while 43% use ICT resources such as computers to teach. 67% of the respondents did not know what a firewall is. Also, 60% of the respondents specified that they use computers on a weekly basis. 52% of the respondents had attained a diploma and 72% had no training on basic computer packages. Table 4 below summarizes the qualification level of the respondents.

Characteristics	% of Respondents
Academic Qualifications	
Masters	11%
Bachelor	37%
Diploma	52%
Basic computer packages training	
Yes	28%
No	72%

Table 4: Qualification level of respondents

c. MANAGEMENT SUPPORT

44% of the respondents reported that their school had an officially authorized contact person in case an information security adversity such as hacking or infection with malicious software was encountered. 67% indicated that their school managements did not have an information security team put in place.

d. INFORMATION SECURITY POLICY AND RISK MANAGEMENT

55% of the respondents agreed that the principal is responsible for information security at the school while 45% felt that the IT department head is responsible for the same. 84% of the respondents indicated that their school did not have a formal information security policy. Also, 62% reported that their school performed regular workplace and information checks and 72% felt that their internet service provider or official ICT authorized contact was competent and trustworthy to secure the school's workspace.

INFORMATION SECURITY AWARENESS

60% of the respondents agreed that avenues for learning about information security were lacking and 66% agreed that teachers should receive information security awareness education. Only 35% indicated that they knew the measures to take to ensure information security. Table 5 below summarizes the perceptions of respondents.

Question	Disagree strongly	Disagree	Difficult to say	Agree	Agree Strongly
Should teachers receive information security awareness education?	7%	3%	12%	12%	66%
Should schools avail more opportunities for information security awareness training for the employees?	8%	8%	14%	9%	61%
Should the government provide more opportunities for information security awareness training for the teachers?	6%	4%	8%	16%	66%
Do you think that Information security awareness programs are not needed if security software is used?	36%	15%	22%	14%	13%
Do you know the measures that you should take to ensure information security?	16%	16%	33%	17%	18%
Do you think that there is lack of training avenues to learn about information security?	13%	6%	21%	8%	52%

Table 5: Responses on Information Security Awareness

MATHEMATICAL REGRESSION ANALYSIS FINDINGS

The SPSS procedure Regression helps in understanding how the value of the dependent variable changes when any of the independent variables is varied while the other independent variables remain fixed.

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.212[a]	.45	.50	.176

a. Predictors: (Constant), FACT4, FACT6, FACT3, STA2, STA1,FACT2, FACT5, FACT1, STA3

Table 6: Model Summary

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.168	8	.021	.677	.0048[b]
	Residual	3.472	113	.030		
	Total	3.901	121			

a. Dependent Variable: SECAWARE

b. Predictors: (Constant), FACT4, FACT6, FACT3, STA2, STA1, FACT2, FACT5, FACT1, STA3

Table 7: ANOVA[a] table

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	2.125	.215		9.877	.000
FACT1	.014	.062	.022	.226	.0036
FACT5	.095	.053	.170	1.803	.0028
STA1	.098	.056	.169	1.900	.0029
1 STA3	.038	.048	.082	.261	.0032
FACT2	-.014	.049	-.027	-.279	.781
FACT3	-.008	.022	-.033	-.358	.721
STA2	.040	.051	.059	.629	.0040
FACT4	.033	.043	.071	.771	.0044

a. Dependent Variable: SECAWARE

Table 8: Coefficients Table

V. DISCUSSION

STATUS OF INFORMATION SECURITY AWARENESS

a. ACCESS TO INFORMATION SECURITY EDUCATION

None of the respondents had received any information security training at their place of work or seminars; this shows there is lack of access to information security education for the teachers. These should be organized by the Ministry of Education and the Teachers Service Commission. This is important as teachers need to enhance their status of information security awareness. Time must be allocated to make teachers aware of information security best practices. Information security awareness begins with teaching individuals how to protect their personal information.

b. BASIC INFORMATION SECURITY PRACTICES

Majority of the teachers had little or no knowledge of basic information security practices such as creating strong passwords, using password-protected screensavers, logging off the computer while away from the workstation, and protecting personal data; this is quite alarming given that the adoption of ICT in teaching and learning has been on the rise. It is vital to educate the teachers on information security to make them aware of best security practices to ensure information security.

ISSN: 2394-4404

c. BASIC KNOWLEDGE OF INFORMATION SECURITY ROLES, THREATS, RISKS AND ATTACKS

It is worrying that secondary school teachers in Kisumu County are yet to fully understand the risks posed by ICT such as hacking, identity theft, phishing, data leakage and other forms of cyber-attacks which can cause delays or temporarily halt execution of critical administrative functions; the protection of a school's ICT assets cannot be overemphasized. Most teachers felt that security measures were an organizational responsibility and not an individual responsibility. This is a misconception as every person has a role to play in ensuring safety of data in the institution. Most cyber criminals prey on human errors and weaknesses for successful security attacks hence it is vital that teachers are educated on their individual and collective roles in protecting sensitive data from unauthorized access and also on what would happen in case of a successful cybercrime attack.

FACTORS THAT AFFECT INFORMATION SECURITY AWARENESS

a. ICT INFRASTRUCTURE, RESOURCES AND PERSONNEL

Respondents from schools with adequate ICT infrastructure, resources and personnel as well as with a formal information security policy appeared to be more knowledgeable about information security practices. The availability of computers, software applications and internet connection remains quite unaffordable to most Kenyan public secondary schools and this may affect information security awareness as it means teachers have little or no exposure to modern ICT resources. As the County Government develops an Information Security Awareness Policy and rolls out information security awareness training programs for teachers, it should as well provide more ICT resources and personnel to schools with greater attention to internet connection and information security applications such as firewalls and anti-virus software.

b. TECHNICAL KNOWLEDGE/SKILLS IN ICT AND QUALIFICATION LEVEL

With information security incidents on the rise, one would expect that as teachers adopt ICT usage, they would be more cautious about internet access and proper computer use. Also, the respondents' qualification level did not significantly influence their knowledge of information security. As such, information security knowledge did not depend on an individual's qualification level. Regrettably, some respondents seem ignorant despite having some knowledge about information security and this increases vulnerability to information security attacks. Furthermore some teachers have negative attitudes towards technology, consequently reducing the desire to learn or be aware about information security issues.

c. MANAGEMENT SUPPORT

Personal or sensitive data, software applications, networks, computers, and school websites are vital assets for an institution and any breaches could have disastrous consequences. The school management is an important player in information security awareness and properly trained ICT personnel, who should be in charge of information security awareness should be hired in schools. The management should also put up ICT security teams headed by an ICT manager or technician who should oversee the implementation of the information security awareness policy, address any concerns about information security and be answerable to the principal who is the secretary to the school's board of management. However, for the management to incorporate such a position funding by the government would be required, further justifying the need for government intervention. Management support is positively related to the overall institution's security culture (Ojwang, 2012).

d. INFORMATION SECURITY POLICY AND RISK MANAGEMENT

Respondents from the few schools with a formal information security policy seemed to be well informed about basic information security practices hence greater information security awareness. An information security awareness policy provides guidelines relating to aspects such as browsing, information transfer and logins, to ensure data protection of sensitive data and providing a broad understanding of information security threats, risks and best practices. The County Government should develop a wide-ranging information security awareness policy that would be mandatory in every public secondary school with ICT resources. A county-wide policy would ensure uniform or near uniform implementation of the policy.

INFORMATION SECURITY AWARENESS

Learning about information security is important and the Government and schools should provide more opportunities for the training initiatives. The training would involve aspects such as technical skills in ICT, software use, internet usage, information storage and protection, identification of information security threats, and response to information security threats. This is a critical as institutions with information security awareness programs and training initiatives are more likely to have members of staff that have greater information security awareness. Most public secondary schools do not have the resources to offer this training, hence the need for Government intervention.

MATHEMATICAL REGRESSION ANALYSIS MODEL

The regression formula is Y= c+b1x1+b2x2+b3x3+b4x4+b5x5+b6x6+b7x7+ b8x8+e where Y is information security awareness the dependent variable coded as SECAWARE while x1 is ICT infrastructure, resources and personnel, x2 is technical knowledge/skills in ICT, x3 is qualification level, x4 is management support, x5 is

information security policy and risk management, x6 is access to information security education, x7 is basic information security practices and x8 is basic knowledge of information security roles, threats, risks and attacks; these are the eight independent variables coded as FACT1, FACT2, FACT3, FACT4, FACT5, STA1, STA2 and STA3 respectively; c is the constant and e is the error term; b1, b2, b3, b4, b5, b6, b7 and b8 represent the coefficient for each independent variable and reflects the relationship between the dependent and independent variables.

a. MODEL SUMMARY

From table 6, R represents the multiple correlation coefficient and is a measure of the quality of the prediction of the dependent variable. R of 0.212 shows a positive but low degree of prediction. The R Square value 0.45 indicates total variations in the dependent variable which can be explained by the eight independent variables; the model can explain up to 45% of variations in the dependent variable, information security awareness.

b. ANOVA TABLE

From table 7, the p-value obtained (0.0048) is less than the alpha value (0.05), which indicates that the model statistically significantly predicts the outcome and that it is a good fit for the data, with a total degree of freedom of 121 degrees.

c. COEFFICIENTS TABLE

Table 8 tests the statistical significance of each variable shown in Sig column; information security policy and risk management (FACT5) was the most significant variable in the model with a p-value of 0.0028. Qualification level (FACT3) and Technical skills/knowledge in ICT (FACT2) have p values of 0.721 and 0.781 respectively which are higher than the alpha value 0.05 hence they are not statistically significant in the model.

The regression analysis model can therefore be summarized as follows:

Y=2.125+(x1*0.014) +(x2*0.014) +(x3*0.008) +(x4*0.033) +(x5*0.095) +(x6*0.098) +(x7*0.040) +(x8*0.038) + e

Y is the dependent variable, information security awareness with an R^2 of 0.45 which indicates that the model can explain up to 45% of variations in the dependent variable. Generally, a multiple regression was run to predict SECAWARE from STA1, STA2, STA3, FACT1, FACT2, FACT3, FACT4 and FACT5. These variables statistically significantly predicted SECAWARE, F (8,113) =0.677, $p<0.05$, R2 = .45 Six of the eight variables added statistically significantly to the prediction, $p<0.05$

VALIDATED FRAMEWORK FOR INFORMATION SECURITY AWARENESS

The regression analysis was based on a confidence level of 0.95 hence giving an alpha value of 0.05. The statistical significance values of the variables are shown in table 7 sig column. If the p-value is less than the alpha value ($p<0.05$), there is a statistically significant relationship between the dependent and independent variables and the variables are therefore important in the model; if the p value is higher than 0.05, then there is no statistically significant relationship between the dependent and independent variables. Therefore, six out of the eight variables are statistically significant in the model while qualification level (0.721) and technical knowledge/skills in ICT(0.781) are not statistically significant. The R^2value is 0.45 showing the total variations in the dependent variable (information security awareness) which can be explained by the independent variables; the model can explain up to 45% of variations in the dependent variable. Figure 2 below shows the validated framework.

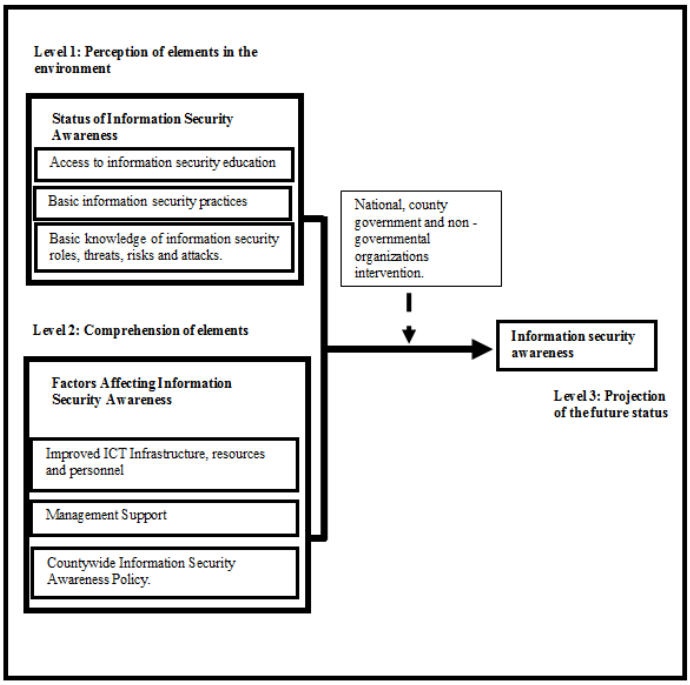

Figure 2: The validated framework for governance of Information Security Awareness

From figure 2 above, Level 1 answers questions such as who is where and which information is needed; it informs on the status of information security awareness. *Level 2* answers questions such as what are they doing or putting in place and what does that mean; Countywide Information Security Awareness Policy, Management Support and Improved ICT Infrastructure, Resources and Personnel should be put in place as they are the main factors affecting information security awareness. Level 3 answers questions such as what will happen in the future and what effect will it have; the future projection is that the developed framework on adoption will ensure increased information security awareness of secondary school teachers of Kisumu County.

VI. CONCLUSION

Despite increased usage of ICT in schools, the status of information security awareness among teachers is even more worrying. With a sample of 172 respondents involving principals and heads of departments, the study which took the

form of a descriptive survey, found that secondary school teachers in Kisumu County had little or no knowledge of basic information security practices. Majority were not aware of what constitutes a strong password, how to protect personal data, the possibility of personal data being used for malicious purposes, and how to store and access data safely. Also, most respondents were not concerned about handling sensitive data, spam mail, and antivirus software. The survey further established that respondents without ICT training and from schools without a formal information security policy and adequate ICT infrastructure were less knowledgeable about basic information security practices.

The developed framework recognizes three levels based on Endsley's theory of situational awareness that would be crucial for the mitigation of information security risks in secondary schools. A fundamental attribute of the framework is the involvement of the Government in raising information security awareness among teachers; developing a Countywide Information Security Awareness Policy; funding Information Security Programs; ensuring school management support and improvement of ICT infrastructure and resources. The Government must ensure that as the framework is implemented it is accepted as adequate not just locally but globally by ensuring that internationally recognized security industry standards are incorporated as the baselines for the framework such as the Security Forum's Standards of Good Practice, The International Standards Organization's Security Management Series (27001, 27002, and 27005) and the Information Systems Audit and Control Association's Control Objectives for Information Technology (COBIT).

VII. RECOMMENDATION

For policy the Government should develop a mandatory county-wide policy to govern information security awareness in public secondary schools in the county and particularly, focus should be on information security awareness training for teachers, the improvement of ICT infrastructure and resources and the installation of Information Security teams headed by an ICT manager or technician in every school. The County Departments of Education should coordinate and supervise the implementation and evaluation of the policy.

For practice administrators and teachers should recognize the importance of learning recommended information security practices and use ICT resources in school in accordance with the developed information security awareness guidelines. Also, teachers should acknowledge that information security is not only an organizational, but also an individual responsibility.

As this study focused on public secondary schools research should therefore be conducted in private secondary schools to ascertain whether there are similar challenges in terms of information security awareness among secondary school teachers.

REFERENCES

[1] Ahlan, A., Lubis, M., & Lubis, A. (2015). Information security awareness at the knowledge-based institution: its antecedents and measures. Procedia Computer Science, 72, 361-373.
[2] Al-Janabi, S., & Al-Shourbaji, I. (2016). A Study of Cyber Security Awareness in Educational Environment in the Middle East. Journal of Information & Knowledge Management 15(01).
[3] Aloul, F. A. (2012). The need for effective information security awareness. Journal of Advances in Information Technology, 3(3), 176-183.
[4] Bryman, A. (2008). Social research methods.3rd ed. Buckingham: Open University Press.
[5] Bulgurcu, B., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 34(3), 523-548.
[6] Chan, H., & Mubarak, S. (2012). Significance of information security awareness in the higher education sector. International Journal of Computer Applications, 60(10).
[7] Curts, R. J., & Campbell, D. E. (2001). Avoiding information overload through the understanding of OODA loops, a cognitive hierarchy and object-oriented analysis and design. Annapolis, MD: C4ISR Cooperative Research Program (CCRP).
[8] Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: A critical study of the content of university policies. International Journal of Information Management, 29(6), 449-457.
[9] Endsley, M. R. (1995). Measurement of situation awareness in dynamic systems. Human Factors:. The Journal of the Human Factors and Ergonomics Society, 37(1), 65-84.
[10] Endsley, M. R. (2016). Designing for situation awareness: An approach to user-centered design. CRC press.
[11] Farooq, A., Isoaho, J., Kakakhel, S, & Virtanen, S. (2015). Information security awareness in educational institution: an analysis of students' individual factors. Internet Technology and Secured Transactions (ICITST) 2015 10th International Conference, pp. 280-286.
[12] Gurney, J. (2014). Lessons in cybersecurity launched for schoolchildren. The Telegraph.
[13] Kiptalam, G. K., & Rodriguez, A. J. (2010). Internet utilization: A case of connected rural and urban secondary schools in Kenya. International journal of computing and ICT research, 4(1), 49-63.
[14] Kenya Open Data Portal, (2014). Secondary Schools by school status and Average Schools Size. The Ministry of Educations' - Basic Education Statistical Booklet.
[15] Kimwele, M., Mwangi, W., & Kimani, S. (2011). Information technology (IT) security framework for Kenyan small and medium enterprises (SMEs). International Journal of Computer Science and Security (IJCSS), 5(1), 39.
[16] Mbogo, G. W., Onunga, A. D., & Kirathi, M. N. (2014). An Evaluation of the Implementation of Information

Technology in Secondary Schools in Kenya. Mediterranean Journal of Social Sciences, 5(5), 215.
[17] Moen, R., & Norman, C. (2006). Evolution of the PDCA cycle.
[18] Mohsen, T., & Dennick, R. (2011). Making Sense of Cronbach's Alpha. International Journal of Medical Education, 2, 53-55. doi:10.5116/ijme.4dfb.8dfd
[19] Oduor, A. (2015 November 08). Kenya National Examination Council rolls out electronic testing, marking system to curb cheating. Standard Media Website. Retrieved 18th August 2016 from: https://www.standardmedia.co.ke/article/2000181929/knec-rolls-out-electronic-testing-marking-system-to-curb-cheating
[20] Ojwang, C. O. (2012). E-learning readiness and e-learning adoption among public secondary schools in Kisumu County, Kenya (Doctoral dissertation).
[21] Okewa, J. J. (2011). Information and communication technology adoption among public secondary schools in Kisumu County, Kenya (Doctoral dissertation).
[22] Okuku, A., Renaud, K., & Valeriano, B. (2015). Cyber security strategy's role in raising Kenyan awareness of mobile security threats. Information & Security, 32(2).
[23] Rajewski, J. (2013, October). Cyber security awareness – why higher education institutions need to address digital threats. Huffington Post. Retrieved from http://www.huffingtonpost.com/jonathan-rajewski/cyber-security-awareness-_b_4025200.html
[24] Stanton, N. A., Chambers, P. R., & Piggott, J. (2001). Situational awareness and safety. Safety science, 39(3), 189-204.
[25] Yamane, T. (1967). Statistics: An Introductory Analysis, 2nd Edition. New York: Harper and Row.