The African Journal of Information Systems

Volume 10 | Issue 3 Article 4

May 2018

Information security awareness amongst students joining higher academic institutions in developing countries: Evidence from Kenya

Joshua R A Ndiege
United States International University-Africa, joshuarumo@yahoo.com

Gabriel O. Okello
United States International University - Africa, gokello@usiu.ac.ke

The African Journal of Information Systems

Information security awareness amongst students joining higher academic institutions in developing countries: Evidence from Kenya

Research Paper

Volume 10, Issue 3, July 2018, ISSN 1936-0282

Joshua Rumo A Ndiege
School of Science and Technology
United States International University – Africa
jrumo@usiu.ac.ke

Gabriel Otieno Okello
School of Science and Technology
United States International University – Africa
gokello@usiu.ac.ke

(*Received October 2017, accepted February 2018*)

ABSTRACT

Although there is a steady use of information technology in institutions of higher learning, little is known about the level of information security awareness (ISA) amongst students joining universities in developing countries and more specifically Africa. The purpose of this study was to investigate ISA amongst undergraduate students at a higher education institution in Kenya. The study made use of a quantitative survey approach. Overall, the study findings indicate that majority of the students surveyed did not possess adequate understanding of ISA. Consequently, we submit that there is a strong need to cultivate ISA culture amongst students joining universities in developing countries. We further recommend that ISA needs to be incorporated in the undergraduate curriculum to help enhance such awareness. Equally, it would be useful for universities to have ISA program as part of the wider university information security management strategy.

Keywords

Information security awareness, academic institution, institutions of higher learning, developing countries, Kenya

INTRODUCTION

In light of the advances and the manner in which information technology (IT) is fast defining the global environment, there is a growing drive in pedagogic discourse on the need to fully integrate IT into the academic environment to support learning and teaching (Facer & Sandford, 2010; Manca & Ranierit, 2016; Chingos, Griffiths, Christine, & Richard, 2017; Assar, Amrani, & Watson, 2010; Akçayır, 2017; Pacheco, Lips, & Yoong, 2018). Consequently, there is a multiplicity of technological solutions being exploited within the educational sector and learners are getting more exposed to such technologies as they join universities (O'Connor & Domingo, 2017; AlTameemy, 2017; Bailey & Brown, 2016; Turney, Robinson, Lee, & Sourtar, 2009). Such usage exposes both the learners and the institutions to myriad of technological threats and exploits. It becomes imperative, therefore, that learners are aware of various information security threats and exploits and how they can safely and securely harness technology without compromising themselves or the institution.

Today, a large number of students joining institutions of higher learning are largely 'digital natives' who have grown up interacting with IT in various facets of their lives (Cerretani, Iturrioz, & Garay, 2016; Kirschner & Bruyckere, 2017; Ting, 2015; Neumann, 2018). It is sensible, therefore, to provide a learning environment that appreciates learners with this background. To this end, universities in both developed and developing countries continue to champion the use of IT within their institutions. In Kenya, for example, the Commission for University Education (CUE) requires universities to establish, implement and maintain IT solutions relating to their core functions (CUE, 2017). This increased usage of IT within academic environment comes with a plethora of new exposures. Consequently, the need to raise information security awareness (ISA) amongst various communities within the academia has never been more important.

Whereas a number of studies demonstrating advancements and gaps on ISA within academia have been done (Adam & Rezgu, 2009; Drevin, Kruger, & Steyn, 2007; Farooq, Isoaho, & Virtanen, 2015; Cox, Connolly, & Currall, 2001; AlTameemy, 2017), the absence of studies which focus on students joining universities in developing countries and more specifically Africa is conspicuously lacking in information security literature. Few attempts to bridge this gap do have direct focus on students joining higher academic institutions (Adam & Rezgu, 2009; Farooq et al., 2015). Furthermore, our literature search on ISA in Kenya on various databases including E-Journals, Academic Search Complete, Education Science, ScienceDirect, Directory of Open Access Journals, Emerald, and Sage Journals amongst others did not yield any result. This is a clear indication that there is need for the research community to carry out studies on ISA in the least researched countries like Kenya.

Taking all these into consideration, the specific objective of this research is to make a contribution to the extant literature on ISA in institutions of higher learning in developing countries. This was done by exploring the level of ISA amongst students joining one of the universities within Nairobi in Kenya.

This section is followed by a literature presentation on ISA with specific attention on how the construct has been conceptualized and defined. A review of ISA in academia is also focused on. The methodological processes adopted in this study are then presented followed by study findings and discussions. We then conclude the paper by making the study summary, limitations and recommendations for future research directions.

LITERATURE REVIEW

Previous studies have indicated that information security awareness (ISA) is key in alleviating risks linked to information security breaches (Safa, Von Solms, & Furnell, 2016). Line users' naivety as well as unintentional behaviour are viewed to be the most frequent causes of information security breaches (Parsons *et al*., 2015; McCormac *et al*., 2017). Therefore, increasing the levels of ISA amongst line users reduces the possibility of them causing information security breaches and consequently improving the efficiency of countermeasures that universities put in place to protect themselves and their constituents against information security related threats and exploits. It is imperative that those who use information technology (IT) resources are knowledgeable on the need for safeguarding information systems and related resources.

ISA can be viewed as the degree of understanding that users have regarding the relevance of information security best practices. Mostly, users will have varying levels of ISA (Farooq *at al*., 2015; McCormac *et al*., 2017). The main focus of ISA is on building sound information security behaviour as part of the overall information security management.

By nature, ISA is an informal and a socially defined construct (Tsohou, Kokolakis, Karyda, & Kiountouzis, 2008). As a result, it has varied definitions within extant literature which translates into a lack of universal understanding of ISA. This has likely exacerbated the level to which the construct has been inconsistently applied. Such inconsistencies may make it challenging for researchers to relate different studies on ISA. It is worth highlighting, that a number of literature on ISA fall short of explicitly defining the term (Banerjee, Banerjee, & Murarka, 2013; Budzak, 2016; Farooq *et al*., 2015). An interestingly surprising fact.

ISA has been widely conceptualized as a cognitive state of mind which is defined by the appreciation of the relevance of information security and being averse with information security objectives, threats as well as associated risks. However, it is apparent from various definitions that ISA is not just about being cognizant of issues related to information security. From the extant literature, the definitions largely fall under three categories: cognitive, behavioural and process. Table 1 provides a summary of these views.

View	Description	Illustrative Reference
Cognitive	From this perspective, ISA is considered as one's state of mind, which is defined by appreciation of the relevance of information security, knowledge about information security threats, risks as well as objectives and ability to use information system rightfully.	Bulgurcu *et al*. (2010); Banerjee *et al*. (2013); D'Arcy, Hovav, and Galletta (2009); and McCormac *et al*. (2017)
Behavioral	In this view, ISA is defined by information security behavior like adherence to security policies and mission amongst others.	Dinev, Goo, Hu, and Nam (2009); Hellqvist *et al*. (2013); and Rotvold and Braathen (2008)
Process	This view takes into consideration various processes or initiatives put in place by organizations to raise ISA.	Tsohou, Karyda, Kokolakis, and Kiountouzis (2009); Lim, Ahmad, and Maynard (2010); Kritzinger and Smith (2008); and Rastogi and Von Solms (2012)

Table 1: Information Security Awareness Views

The use of IT within academia has been widely reported in the literature. In Africa, for example, national developments, and growing favorable policies as well as support systems continue to fuel the use of IT within institutions of higher learning (Carr, 2013; Rambe, 2015). Accordingly, a number of

institutions of higher learning in Africa continue to embrace the use IT to support teaching and learning. As technology permeates the educational sector, so are the threats and vulnerabilities associated with such use.

Information security continues to receive growing attention with various scholars and practitioners giving focus to the subject (Budzak, 2016; Bulgurcu, Cavusoglu, & Benbasat, 2010; Ki-Aries & Faily, 2017; McCormac *et al*., 2017). This is largely attributed to the fact that security is a critical element when developing and implementing IT within institutions. A number of studies have emphasized on the relevance of removing weaknesses in an information security chain. Such weaknesses more often would present itself when people unconsciously or consciously interfere the existing systems. Consequently, there is need for ISA. However, building awareness and changing information security behaviour can be an overwhelming task noting that one must be a live to the reality of the growing threats as well as be knowledgeable on the approaches for identification and mitigation of various information security related threats and attacks (Budzak, 2016; Farooq *et al*., 2015). Most measures employed towards ISA do not always translate into the needed behavioural change (Ki-Aries & Faily, 2017).

IT continues to be a preferred choice as a tool for enhancing learning and teaching in the education sector (AlTameemy, 2017; Assar *et al*., 2010; Chingos *et al*., 2017). And this is not only because universities today receive students who are digital natives, but also since technology is considered to provide greater flexibility with regard to place and time. For example, through technology, students are able to enhance access and learning opportunities on campus as well as off campus.

The usage of IT within universities can range from basic usage like the provision of online access to basic course materials to more advanced usage involving complete integrated learning and teaching system devoid of formal contact between the instructor and learners.

In Kenya, for instance, universities continue to extend their programs to the internet and the need for virtual universities continue to dominate strategic directions of academic institutions (CUE, 2017; Mutisya & Makokha, 2016). This they do to help break geographical barriers and allow equitable access to education. Furthermore, the Kenya Educational Network (KENET) which is the National Research and Educational Network (NREN) of Kenya, has over the years continued to offer affordable, cost-effective and low congestion internet bandwidth services to academic institutions in Kenya (KENET, 2018). This has translated into improved use of IT within institutions of higher learning in Kenya. The Communication Authority of Kenya in their annual report for the financial year 2015-2016 observed that the use of mobile devices in the country increased to 90% edging closer to the average global penetration rate which stood at 98% as at 2015 (Communications Authority of Kenya, 2016).

On the other hand, the National ICT survey conducted by Communication Authority of Kenya in 2010 revealed that use and access of IT equipment and facilities was more widespread among the youth aged between 20 and 34 years (Communication Authority of Kenya, 2018). Considering that this is normally the age that many students join the university, it may be concluded that a good number of the students joining Kenyan universities are technologically literate. The survey further found that more than half of the household population undertaking IT related courses are in primary schools level while 32% are in secondary. This growth in use of technology increases the possibility of IT related threats and exploits.

Although a number of institutions have introduced computer literacy into their curriculum as a general education requirement, the component of information security education is never a requirement. A look at the curriculums of various academic programs offered by universities in Kenyan, the information security education is mainly offered to those students who are enrolled in IT related degree programs (CUE, 2017). Owing to the widespread of cybercriminal activities, learners, irrespective of their career

orientation need to have a good understanding of information security issues in order to safe guard themselves and the institution against possible threats and exploits.

While it is true that universities have IT divisions and may offer certain measures as background service to protect IT resource users, there are instances when decisions made by line users like students have security risk implication (Drevin *et al*., 2007; Parsons *et al*., 2014; Budzak, 2016). In the same way, such risks would be serious in non-academic sector, they would also have negative ramifications in the academic environment.

Within universities, security breach may lead to loss of data, time, as well as reputation to both the institution and the student. It is therefore imperative that students who are one of the key line consumers of technology resources within universities, have a good knowledge of potential threats they are exposing themselves or the institution to and how they can contribute to a secure usage of the IT resources. Further, it is important to be conscious of the fact that there has been a steady rise in security breaches and exploits both regionally and globally in all sectors of the economy (Budzak, 2016; Laybats & Tredinnick, 2016).

To this end, it is important that institutions of higher learning counter user triggered threats and exploits through formulation and implementation of ISA. Additionally, sound information security policies and procedures are needed to positively influence the line users' behavior as they consume IT resources. It is becoming clear that ISA needs to be provided to students at early stages in their academic life. This will better prepare them to pay attention to security issues and avoid getting involved in behavior that could compromise the IT resources within the institutions or make them vulnerable to threats and attacks.

The purpose of this study, therefore, is to make a contribution to the extant literature on ISA in institutions of higher learning in Africa. We do so by investigating the level of ISA amongst students joining one of the universities within Nairobi in Kenya.

METHODOLOGY

In this study we made use of positivist, quantitative research approach. The population of the study consisted all the first year university students who had just joined the university (n=380). Purposive sampling was employed to ensure that only the new first year students participated in the study. Following the administration of the survey, a response rate of 82.9% (315 students returning completed questionnaires) was recorded. This is considered sufficient response (Oates, 2006). To ensure content validity and completeness, the questionnaire was reviewed by two experts (faculty teaching information security program at university) and corrections done based on their feedback. Further, we conducted a pilot study to test for any ambiguity, completeness, and understandability by administering the instrument to a group of 10 first year students. The statements that the participants did not understand were reviewed and revised to refine the instrument.

The questionnaire consisted four parts. In Part 1, student's demographic information was collected. Part 2 was made up of 7 statements that focused on general security awareness on which the respondents were required to respond to using a 4 point Likert scale (1=strongly disagree to 4=strongly agree). In Part 3 we used 9 statements that focused on information security. Part 4 of the questionnaire dwelt on physical security and comprised of 3 statements. As was the case with part 2, the respondents were required to respond through a 4 point Likert scale in parts 3 and 4.

The analysis of the questionnaire items was done using Statistical Package for Social Sciences (SPSS) Version 22 and descriptive statistics (frequencies and percentages) was employed to present the findings. Further, to help make a determination on which category of students were more or less likely to be versed with ISA, the study used logistic regression analysis.

RESULTS

Demographics

In this study we endeavoured to explore the level of information security awareness (ISA) amongst students joining one of the universities within Nairobi in Kenya. Basic demographic results from the study are presented in order to allow the study to be characterized accordingly. Our study sample consisted of 174 (55.2%) females and 141 (44.8%) males. 93.7 percent of the study participants were aged between 16 and 25 years. This is falls within the normal age group because majority of students in universities in Kenya enter these institutions right after high school. Those that were above 26 years comprised the smallest population at only 20 (6.3%). With regard to the type of high school attended, of the sampled students, nearly two-thirds of the participants (192, 61.0%) had attended private schools while 123 (39%) had attended public schools.

Majority of the students sampled (245, 77.8%) indicated they had already done some computer related studies before joining the university with 66.7% of this population indicating that they had done such studies at high school. However, it is clear that such trainings received by the students did not address areas related to ISA as only 12.2% of the students strongly agreed to having received ISA training before.

To understand the level of ISA amongst the participating students, we made use of the following categories: *General security awareness* which consisted of seven questions (see Table 2); *Information security* consisted of nine questions (see Table 3) and *Physical security* comprised of three questions (see Table 4).

General security awareness

On the theme of general security awareness, majority of the students at 97.4% agreed that they understood the requirements for and use of strong password. When asked whether they would share their password online or post it where others may obtain access to it, significantly, 98% said they would never share their password online. Only 17.3% strongly agreed that they know how to protect against computer crime while 19.1% are not keen to access only trusted, reputable sites. Regarding what constitute acceptable use of computers, 20.4% observed they had no knowledge of this, while 50.5% agreed to have knowledge of this. However, only 29.1% strongly agreed to know what constitute acceptable use of computers. Nearly half of the students 48.1% believe that what they do on the computer could not affect others. Nevertheless, it is interesting to note that only 12.2% of the students strongly agreed to have received information security awareness training before.

Information security

On the theme of information security presented on Table 3, majority of the students at 94.2% seems to appreciate what information is considered sensitive. This is further corroborated by 63.8% of the students strongly agreeing that they are careful not to discuss sensitive information in public places.

Statements on the general security awareness	**Levels of agreement**							
	Strongly Disagree		Disagree		Agree		Strongly Agree	
	n	%	n	%	n	%	n	%
I understand the requirements for and use of strong password	2	0.6	6	1.9	98	31.7	203	65.7
I never share my password online or post it where others may obtain access to it	3	1	3	1	54	17.5	248	80.5
I know how to protect against computer crime	25	8.3	109	36.3	114	38	52	17.3
When browsing or downloading from internet, I only access trusted, reputable sites	9	3	49	16.1	124	40.7	123	40.3
I know what constitutes acceptable use of computers	15	5.2	44	15.2	146	50.5	84	29.1
What I do on my computer could affect other people	63	21.2	80	26.9	69	23.2	85	28.6
I have received Information Security awareness training before	71	23.4	120	39.5	76	25.0	37	12.2

Table 2: General Security Awareness

Statements on information security	**Levels of agreement**							
	Strongly Disagree		Disagree		Agree		Strongly Agree	
	n	%	n	%	n	%	n	%
I understand what information is considered sensitive (confidential and proprietary)	7	2.4	10	3.4	127	42.9	152	51.3
I am careful not to discuss sensitive information in public places	5	1.7	8	2.7	94	31.8	189	63.8
I am familiar with the appropriate methods for transmitting, storing, labelling and handling sensitive information	14	4.8	62	21.1	128	43.5	90	30.6
I always encrypt sensitive data when sending via email and I know how/when hardware and mobile devices should be encrypted	36	12.1	115	38.7	101	34.0	45	15.1
I ensure that sensitive data is protected on mobile devices	21	7.2	36	12.3	138	47.1	98	33.4
I do not leave sensitive data unattended in open areas	8	2.7	18	6.1	126	43.0	141	48.1
My sensitive data is backed up on a routine basis	17	5.9	52	18.1	121	42.2	97	33.8
I am aware that texting or posting sensitive data on social sites may violate policy or regulations	6	2.0	11	3.7	109	37.1	168	57.1
I can play a significant role in protecting my computer and the information stored on it	10	3.4	16	5.4	117	39.7	152	51.5

Table 3: Information Security

However, only 30.6% strongly agreed to be familiar with the appropriate methods for transmitting, storing, labelling and handling sensitive information. Half of the respondents, 50.8%, always encrypt sensitive data when sending through email and are knowledgeable on how or when hardware and mobile devices should be encrypted. It is worth noting that of the 50.8% only 15.1% strongly agreed to always encrypting sensitive data. This can be validated by the fact that only 33.4% strongly agreed that they ensure sensitive data on their mobile devices is protected. Again, while 43% agreed that they do not

leave sensitive data unattended in open areas only 48.1% strongly agreed to this and a further 33.8% strongly agreeing that their sensitive data is backed up on a routine basis. Regarding texting or posting sensitive data on social sites, 94.2% believe this act may violate policy or regulations. It is also interesting to note that many students, 91.2% believe they can play a significant role in protecting their computers and information stored in them.

Physical or resource security

Regarding physical or resource security presented in Table 4, while slightly more than half of the respondents at 54% agreed that they do physically secure their mobile devices, only 31.6% strongly agreed to this. In addition, only 22.8% disagreed that their computing devices are current with virus protection. When asked if approved to use their personal computing they are aware of and use security measures, while 53.4% agreed to this, only 31% indicated strongly to be of this view.

Statements on the physical/ resource security	**Levels of agreement**							
	Strongly Disagree		Disagree		Agree		Strongly Agree	
	n	%	n	%	n	%	n	%
I physically secure my mobile computing devices	13	4.6	28	9.8	154	54.0	90	31.6
My computing devices (i.e. laptop, smartphone, desktop) are current with virus protection	16	5.6	49	17.2	126	44.2	94	33.0
If approved to use my personal computing devices, I am aware of and use security measures	12	4.3	32	11.4	150	53.4	87	31.0

Table 4: Physical/Resource Security

We further made use of logistic regression analysis to find out which category of students would more likely be aware of the information security issues using Odds Ratio (OR) and p-values on various ISA areas. These are presented in Tables 5-13.

Regression analysis

Regarding the theme on general security awareness, more male students tend to be more informed on general information security awareness issues than their female counterparts. This was however not significant in most cases as revealed in Table 5. It is however worth observing that male students were significantly more likely to know how to protect against computer crime compared to their female colleagues (OR=2.156094; P-Value=0.0001).

Students who had attended private school tended to be less informed on general information security awareness issues than those from public schools as presented in Table 7. While this was not significant in most cases, students from private school were significantly more likely to know how to protect against computer crime compared to those from public school (OR=1.694276; P-Value=0.024).

Regarding information security, male students appeared to be more knowledgeable on various aspects of information security compared to the female students as indicated in Table 8.

In relation to students who had done computer studies as presented in Table 9, it was evident, that those with computer studies background were more versed with information security matters compared to their counterparts who had no such background.

Statements on the general security awareness		**OR (p-value)**
I understand the requirements for and use of strong password	Female	1.00 (Ref)
	Male	2.31135 (0.159)
I never share my password online or post it where others may obtain access to it	Female	1.00 (Ref)
	Male	1.868182 (0.307)
I know how to protect against computer crime	Female	1.00 (Ref)
	Male	2.156094 (0.001)
When browsing or downloading from internet, I only access trusted, reputable sites	Female	1.00 (Ref)
	Male	.6826241 (0.162)
I know what constitutes acceptable use of computers	Female	1.00 (Ref)
	Male	1.596774 (0.073)
What I do on my computer could affect other people	Female	1.00 (Ref)
	Male	1.232571 (0.357)
I have received Information Security awareness training before	Female	1.00 (Ref)
	Male	1.082336 (0.737)

Table 5: Cross Tabulation on General Security Awareness based on Gender

Statements on information security	**Background**	**OR (p-value)**
I understand the requirements for and use of strong password	No IT background	1.00 (Ref)
	IT background	.869403 (0.832)
I never share my password online or post it where others may obtain access to it	No IT background	1.00 (Ref)
	IT background	1.052239 (0.940)
I know how to protect against computer crime	No IT background	1.00 (Ref)
	IT background	2.864876 (0.000)
When browsing or downloading from internet, I only access trusted, reputable sites	No IT background	1.00 (Ref)
	IT background	1.190493 (0.585)
I know what constitutes acceptable use of computers	No IT background	1.00 (Ref)
	IT background	1.444406 (0.211)
What I do on my computer could affect other people	No IT background	1.00 (Ref)
	IT background	.9444444 (0.833)
I have received Information Security awareness training before	No IT background	1.00 (Ref)
	IT background	1.670965 (0.086)

Table 6: Cross Tabulation on General Security Awareness based on Previous IT studies

Statements on the general security awareness		**OR (p-value)**
I understand the requirements for and use of strong password	Public	1.00 (Ref)
	Private	.7711864 (0.643)
I never share my password online or post it where others may obtain access to it	Public	1.00 (Ref)
	Private	.9745763 (0.965)
I know how to protect against computer crime	Public	1.00 (Ref)
	Private	1.694276 (0.024)
When browsing or downloading from internet, I only access trusted, reputable sites	Public	1.00 (Ref)
	Private	.9287941 (0.792)
I know what constitutes acceptable use of computers	Public	1.00 (Ref)
	Private	.9222476 (0.757)
What I do on my computer could affect other people	Public	1.00 (Ref)
	Private	1.316129 (0.236)
I have received Information Security awareness training before	Public	1.00 (Ref)
	Private	1.131641 (0.609)

Table 7: Cross Tabulation on General Security Awareness based on type of school attended

As presented in Table 10, majority of the students who had attended private schools seemed to be more knowledgeable in information security matters compared to their counterparts who were from public schools. While this was not significant, those from private schools seemed to significantly always encrypt sensitive data when sending it through email and understand how and or when hardware and mobile devices should be protected (OR=1.595395; P-Value-0.046).

Statements on information security		**OR (p-value)**
I understand what information is considered sensitive (confidential and proprietary)	Female	1.00 (Ref)
	Male	1.31297 (0.452)
I am careful not to discuss sensitive information in public places	Female	1.00 (Ref)
	Male	1.206948 (0.620)
I am familiar with the appropriate methods for transmitting, storing, labeling and handling sensitive information	Female	1.00 (Ref)
	Male	1.479374 (0.116)
I always encrypt sensitive data when sending via email and I know how/when hardware and mobile devices should be encrypted	Female	1.00 (Ref)
	Male	1.443717 (0.107)
I ensure that sensitive data is protected on mobile devices	Female	1.00 (Ref)
	Male	1.176136 (0.537)
I do not leave sensitive data unattended in open areas	Female	1.00 (Ref)
	Male	1.049563 (0.878)
My sensitive data is backed up on a routine basis	Female	1.00 (Ref)
	Male	1.089436 (0.728)
I am aware that texting or posting sensitive data on social sites may violate policy or regulations	Female	1.00 (Ref)
	Male	1.130757 (0.726)
I can play a significant role in protecting my computer and the information stored on it	Female	1.00 (Ref)
	Male	1.458824 (0.251)

Table 8: Cross Tabulation on Information Security based on Gender

Statements on information security	**Background**	**OR (p-value)**
I understand what information is considered sensitive (confidential and proprietary)	No IT background	1.00 (Ref)
	IT background	.671875 (0.397)
I am careful not to discuss sensitive information in public places	No IT background	1.00 (Ref)
	IT background	.7896635 (0.619)
I am familiar with the appropriate methods for transmitting, storing, labelling and handling sensitive information	No IT background	1.00 (Ref)
	IT background	1.700483 (0.060)
I always encrypt sensitive data when sending via email and I know how/when hardware and mobile devices should be encrypted	No IT background	1.00 (Ref)
	IT background	1.094804 (0.740)
I ensure that sensitive data is protected on mobile devices	No IT background	1.00 (Ref)
	IT background	1.148693 (0.652)
I do not leave sensitive data unattended in open areas	No IT background	1.00 (Ref)

	IT background	1.201149 (0.615)
My sensitive data is backed up on a routine basis	No IT background	1.00 (Ref)
	IT background	.9530075 (0.870)
I am aware that texting or posting sensitive data on social sites may violate policy or regulations	No IT background	1.00 (Ref)
	IT background	.9247319 (0.853)
I can play a significant role in protecting my computer and the information stored on it	No IT background	1.00 (Ref)
	IT background	1.664063 (0.150)

Table 9: Cross Tabulation on Information Security based on Previous IT studies

Statements on information security	**Type of school**	**OR (p-value)**
I understand what information is considered sensitive (confidential and proprietary)	Public	1.00 (Ref)
	Private	1.130952 (0.732)
I am careful not to discuss sensitive information in public places	Public	1.00 (Ref)
	Private	1.24159 (0.566)
I am familiar with the appropriate methods for transmitting, storing, labelling and handling sensitive information	Public	1.00 (Ref)
	Private	1.291582 (0.303)
I always encrypt sensitive data when sending via email and I know how/when hardware and mobile devices should be encrypted	Public	1.00 (Ref)
	Private	1.595395 (0.046)
I ensure that sensitive data is protected on mobile devices	Public	1.00 (Ref)
	Private	1.084873 (0.759)
I do not leave sensitive data unattended in open areas	Public	1.00 (Ref)
	Private	1.25817 (0.469)
My sensitive data is backed up on a routine basis	Public	1.00 (Ref)
	Private	.9465116 (0.827)
I am aware that texting or posting sensitive data on social sites may violate policy or regulations	Public	1.00 (Ref)
	Private	1.663462 (0.143)
I can play a significant role in protecting my computer and the information stored on it	Public	1.00 (Ref)
	Private	1.116453 (0.734)

Table 10: Cross Tabulation on Information Security based on type of school attended

Regarding physical security, again male students were more knowledgeable on issues related to physical security compared to their female counterparts as presented in Table 11.

Further, as captured in Table 12, students with computer studies background were more versed with physical security issues compared to those who had not such background. However, this was not significant.

Similarly, majority of students from private schools seemed to be more acquainted with physical resource security compared to those students who came from public schools as presented in Table 13.

Statement on physical/resource Security	Gender	OR (p-value)
I physically secure my mobile computing devices	Female	1.00 (Ref)
	Male	.9840278 (0.953)
My computing devices (i.e. laptop, smartphone, desktop) are current with virus protection	Female	1.00 (Ref)
	Male	1.320513 (0.265)
If approved to use my personal computing devices, I am aware of and use security measures	Female	1.00 (Ref)
	Male	1.224121 (0.445)

Table 11: Cross Tabulation on Physical/Resource Security and Gender

Statement on physical/resource Security	Background	OR (p-value)
I physically secure my mobile computing devices	No IT background	1.00 (Ref)
	IT background	.9204549 (0.801)
My computing devices (i.e. laptop, smartphone, desktop) are current with virus protection	No IT background	1.00 (Ref)
	IT background	.8284314 (0.533)
If approved to use my personal computing devices, I am aware of and use security measures	No IT background	1.00 (Ref)
	IT background	.9675224 (0.917)

Table 12: Cross Tabulation on Physical/Resource Security based on Previous IT studies

Statement on physical/resource Security	Type of school	OR (p-value)
I physically secure my mobile computing devices	Public	1.00 (Ref)
	Private	.8096717 (0.452)
My computing devices (i.e. laptop, smartphone, desktop) are current with virus protection	Public	1.00 (Ref)
	Private	1.127551 (0.632)
If approved to use my personal computing devices, I am aware of and use security measures	Public	1.00 (Ref)
	Private	1.284985 (0.344)

Table 13: Cross Tabulation on Physical/Resource Security based on type of school attended

DISCUSSION

The wide spread use of information technology (IT) in institutions of higher learning has no doubt led to a number of information security related challenges. It is evident from the extant literature that issues related to information security awareness (ISA) has continued to draw attention not only from the scholars but also the practitioners (Bailey & Brown, 2016; Farooq *et al*., 2015). It is therefore true that the relevance of ISA cannot be understated. Understanding the level of ISA amongst students joining

institutions of higher learning is critical in helping set the stage for presenting a case on the need for ISA training programs during the first year of students' studies at the university.

The findings from this study demonstrates that the students joining institutions of higher learning in developing countries have varied levels of understanding of ISA with a number of them revealing that they do not have a strong understating of various aspects of ISA. For example, of the seven elements on general security awareness, in only two aspects that revolved around use of password did we have over 50% of the respondents strongly indicate that they were knowledgeable on these aspects. For the other five items under general security awareness, those who strongly agreed fell way below 50%. This relatively high level of ISA on password use could be linked to the fact that password are the most common method of authentication today (Furnell & Esmael, 2017). On information security theme, of the 9 criteria that were tested, only in four did over 50% of the respondents indicate strongly that they were versed with the elements. And on physical or resource security, the respondents who strongly agreed they were versed with the elements on this theme fell way short below 50%. However, Forte and Power (2007) observe that physical security is equally a critical component of information security management and need not be overlooked.

From the aforegoing discussions, it is clear that, it cannot be strongly concluded that these students have sufficient levels of ISA. This lack of awareness was further demonstrated in this study where only 12.2% of the study participants strongly agreeing to have received ISA training before. Such inadequacy was also reported by Adam and Rezgu (2009). Furnell and Vasileiou (2017) paints the current picture on ISA by arguing that, so far, not enough is being done to raise the levels of ISA and that many security exploits are being experienced as a result of this minimal knowledge on ISA.

Students admitted in institutions of higher learning have heterogeneous backgrounds, this seemed to be playing out in their varying levels of understanding of various information securities issues under several themes that were looked at in this study. Previous literature have suggested that students' background has an influence on their technological savviness (Farooq *et al*., 2015; Mutisya & Makokha, 2016). This was found to be true in this study as the findings revealed that students who had previous computer studies background were more versed with ISA compared to their counterparts who did not have such background.

Whereas there can never be one stop solution to information security challenges, ISA is generally considered to be amongst the most effective security methods. A number of studies reveal that the challenge of ISA has not been properly addressed since many IT users do not have adequate security training (Budzak, 2016; Farooq *et al*., 2015). In this study a significant number of students indicated that they had not received ISA training before. This is despite of the fact that a number of high schools (which are feeders to institutions of higher learning) in Kenya have introduced computer studies (Ministry of Education, 2016). This could be explained by the fact that ISA is not given much attention in these curriculums. With the majority of the students joining institutions of higher learning considered as digital natives it will be sensible if adequate training is offered to them on ISA as a way of addressing various security challenges.

This study findings further reveal that female students were less knowledgeable than their male counterparts on various ISA themes that were the focus of this study. A study by Mahmood and Bokhari (2012) on gender difference in IT use amongst students at tertiary level of education reveal that gender

difference does exist in IT use. It would be meaningful, therefore, that efforts to cultivate ISA culture are tailored to address such disparities.

Students from private schools appeared more versed with ISA than those from public schools. It is worth noting that this scenario could largely have been contributed by the fact that most private schools in Kenya are better equipped with IT resources compared to those that are run by the government. Students from private schools start engaging with IT much earlier than their counterparts from public schools. Such exposures naturally render students from private schools better advantaged as far as protection from IT related threats and exploits is concerned. In a summative evaluation of secondary schools, the Kenya Institute of Curriculum Development (2017) observed that not only did the majority of schools have inadequate ICT infrastructure, there was also limited integration of ICT in pedagogy.

Jansson and Von Solms (2013) observe that students can learn and positively adapt to ISA culture. This was found to be largely true as a majority of the students acknowledged that they can be active players in the protection of IT resources. It therefore holds, that students are receptive to learning ISA culture. With proper training and education on ISA, students in institutions of higher learning will be better prepared to deal with IT related threats.

As demonstrated in the extant literature (Budzak, 2016; Ki-Aries & Faily, 2017; Kritzinger & Smith, 2008), a number of studies continue to reveal that improving ISA of users remains one of the most effective methods of information security management. Early training at the entry level at the university will ensure that the students shape their way of thinking on ISA early enough thereby improving the likelihood that they would safely and securely exploit various IT resources within and outside the academic environment.

SUMMARY

The extant literature reveal that there is proliferation in the use of information technology (IT) within institutions of higher learning. Such widespread usage of technology provides additional avenues for exploits and increases the widespread of the impacts of information security breach. Due to the amount of time spent using various IT resources, the student population remain at increasingly high risk to various information security related threats and exploits.

Taken together, these results suggest that it cannot be concluded that students joining institutions of higher learning possess adequate understanding of information security awareness (ISA). Improving ISA of university students is a critical component of the overall approach to information security management. For universities to be able to manage and reduce information security threats, building a strong ISA culture remains critical. The increased ISA amongst the students would translate into a reduction of the probability of unintentional breaches as well as increase the likelihood of the identification and reporting of suspicious activities.

We therefore submit that in contemporary society, institutions of higher learning need to generate ISA as a way of safeguarding against information security breach. There is adequate evidence suggesting that security awareness training is one of the most effective ways of realizing security control. It is therefore imperative that institutions of higher learning develop Security Education Training and Awareness (SETA) programs and make deliberate efforts to ensure that such programs are directed towards students right from the time they join universities.

LIMITATIONS AND RECOMMENDATIONS

With paucity of empirical studies on ISA within institutions of higher learning in developing countries, this study contributed to the understanding of ISA within institutions of higher learning in Africa. It further provides practical contribution to academia. However, despite these contributions, the study limitations must be acknowledged.

Firstly, this study is focused on a single institution of higher learning within Nairobi in Kenya. This has the potential of affecting the generalizability of the results. Secondly, the study sample size used was relatively small as it was a single case study. Further insights could be gleaned through a study that uses a larger sample size involving multiple cases. And finally, on the study limitation, the study respondents were restricted to first year students. Whereas this was purposeful as first year students were the focus of the study, studies on ISA on various populations within institutions of higher learning in developing countries will no doubt enhance the understanding of ISA.

Further, studies on how best the content of SETA programs should be developed in view of the heterogeneity of the students' background would be useful for the successful implementation of such training and awareness programs. There is need to ensure that such programs meet the varying level of technological savviness of the new entrants into the institutions of higher learning. Additionally, such programs should ensure that the inequalities that currently exist based on gender and educational background of the students and their knowledge on ISA are bridged. We further recommend that ISA needs to be incorporated in the undergraduate curriculum to help enhance such awareness. Equally, it would be useful for universities to have ISA program as part of the wider university information security management strategy.

This study sets a good ground to make a case for the need to re-examine the current educational models in institutions of higher learning in developing countries to help make a determination whether the current models are a good fit to address the emerging ISA challenges.

REFERENCES

Adam, M., & Rezgu, Y. (2009). A comparative study of information security awareness in higher education based on the concept of design theorizing. 2009 *International Conference on Management and Service Science*, 1-7, Wuhan, China : IEEE .

Akçayır, G. (2017). Why do faculty members use or not use social networking sites for education? *Computers in Human Behavior*, 71, 378-385.

AlTameemy, F. (2017). Mobile phones for teaching and learning: Implementation and students' and teachers' attitudes. *Journal of Educational Technology Systems*, 45, 3, 436-451.

Assar, S., Amrani, R. E., & Watson, R. T. (2010). ICT and education: A critical role in human and social development. *Information Technology for Development*, 16, 3, 151-158.

Bailey, T. L., & Brown, A. (2016). Online student services: Current practices and recommendations for implementation. *Journal of Educational Technology Systems*, 44, 4, 450-462.

Banerjee, C., Banerjee, A., & Murarka, P. D. (2013). An improvised software security awareness model. *International Journal of Information, Communication and Computing Technology*, 1, 2, 43-48.

Budzak, D. (2016). Information security – The people issue. *Business Information Review*, 32, 2, 85–89.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Qauarterly*, 34, 3, 523-527.

Carr, T. (2013). e/merging across Africa: Five papers on the use of educational technology in African higher education. *The African Journal of Information Systems*, 5, 3, 65-70.

Cerretani, P. I., Iturrioz, E. B., & Garay, P. B. (2016). Use of information and communications technology, academic performance and psychosocial distress in university students. *Computers in Human Behavior*, 56, 119-126.

Chingos, M. M., Griffiths, R. J., Christine, M., & Richard, R. S. (2017). Interactive online learning on campus: Comparing students outcomes in hybrid and traditional courses in the university system of Maryland. *The Journal of Higher Education*, 88, 2, 210-233.

Commission for University Education. (2017, September 20). News Updates. Retrieved from News and Events: http://www.cue.or.ke/index.php/news-and-events

Communication Authority of Kenya. (2018). Publications: Communication Authority of Kenya. Retrieved March 8, 2018, from Communication Authority of Kenya Web site: www.ca.go.ke/images//downloads/universal_access/survey/National%20ICT%20Survey.pdf

Communications Authority of Kenya. (2016, December). Annual Reports. Retrieved March 8, 2018, from CAK Publications: http://www.ca.go.ke/index.php/annual-reports

Cox, A., Connolly, S., & Currall, J. (2001). Raising information security awareness in the academic setting. *VINE*, 31, 2, 11-16.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrance approach. *Information Systems Research*, 20, 1, 79-98.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: The role of national cultural differences. *Information Systems Journal*, 19, 4, 391-412.

Drevin, L., Kruger, H. A., & Steyn, T. (2007). Value-focused assessment of ICT security awareness in an academic environment. *Computers & Security*, 26, 1, 36-43.

Facer, K., & Sandford, R. (2010). The next 25 years? Future scenarios and future directions for education and technology. *Journal of Computer Assisted Learning*, 26, 1, 74-93.

Farooq, A., Isoaho, J., & Virtanen, S. (2015). Information security awareness in educational institution: An analysis of students' individual factors. *14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, 352-359. Helsinki, Finland: IEEE.

Forte, D., & Power, R. (2007). Physical security – overlook it at your own peril. *Computer Fraud & Security*, 2007, 8, 16-20.

Furnell, S., & E. R. (2017). Evaluating the effect of guidance and feedback upon password compliance. *Computer Fraud & Security*, 2017, 1, 5-10.

Furnell, S., & Vasileiou, I. (2017). Security education and awareness: just let them burn? *Network Security*, 2017, 12, 5-9.

Hellqvist, F., Ibrahim, S., Jatko, R., Andersson, A., & Hedström, K. (2013). Getting their hands stuck in the cookie jar - Students' security awareness in 1:1 laptop schools. *International Journal of Public Information Systems*, 2013, 1, 1-19.

Jansson, K., & Von Solms, R. (2013). Phishing for phishing awareness. *Behaviour and Information Technology*, 36, 6, 584-593.

KENET. (2018, March 7). Home. Retrieved March 7, 2018, from Kenya Educational Network: https://www.kenet.or.ke/

Kenya Institute of Curriculum Development. (2017, September 20). Home. Retrieved from Secondary Summative Evaluation: http://kicd.ac.ke/93-departments/153-secondary-summative-evaluation.html

Ki-Aries, D., & Faily, S. (2017). Persona-centred information security awareness. *Computers & Security*, 70, 663-674.

Kirschner, P. A., & Bruyckere, P. D. (2017). The myths of the digital native and the multitasker. *Teaching and Teacher Education*, 67, 135-142.

Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computer & Security*, 27, 5-6, 224-231.

Laybats, C., & Tredinnick, L. (2016). Information Security. *Business Information Review*, 33, 2, 76-80.

Lim, J. S., Ahmad, A., & Maynard, S. (2010). Embedding information security culture: Emerging concerns and challenges. *Proceedings of the 15th Pacific Asia Conference on Information Systems* (PACIS). Australia, Brisbane.

Mahmood, A., & Bokhari, N. H. (2012). Use of information and communication technology: Gender differences among students at tertiary level. *Journal of Educational and Instructional Studies*, 2, 4, 100-108.

Manca, S., & Ranierit, M. (2016). Is facebook still a suitable technology-enhanced learning environment? An updated critical review of the literature from 2012-2015. *Journal of Computer Assisted Technology*, 32, 6, 503-528.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness, *Computers in Human Behavior*, 69, 151-156.

Ministry of Education. (2016, January 1). Digital Learning Program. Retrieved June 22nd, 2017, from Ministry of Education: http://www.education.go.ke/index.php/programmes/digital-learning-programme

Mutisya, D. N., & Makokha, G. L. (2016). Challenges affecting adoption of e-learning in public universities in Kenya. *E-Learning and Digital Media*, 13, 3-4, 140-157.

Neumann, M. M. (2018). Using tablets and apps to enhance emergent literacy skills in young children. *Early Childhood Research Quarterly*, 42, 239-246.

O'Connor, E. A., & Domingo, J. (2017). A practical guide, with theoretical underpinnings, for creating effective virtual reality learning environments. *Journal of Educational Technology Systems*, 45, 3, 343-364.

Pacheco, E., Lips, M., & Yoong, P. (2018). Transition 2.0: Digital technologies, higher education, and vision impairment. *The Internet and Higher Education*, 37, 1-10.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2014). A study of information security awareness in Australian government organizations. *Information Management & Computer Security*, 22, 4, 334-345.

Parsons, K., Young, E., Butavicius, M., McCormac, A., Pattinson, M., & Jerram, C. (2015). The influence of organisational information security culture on cybersecurity decision making. *Journal of Cognitive Engineering and Decision Making: Special Issue on Cybersecurity Decision Making*, 9, 2, 117-129.

Rambe, P. (2015). The role of educational technology in design and delivery of curricula programmes: A case of STEPS at a University of Technology. *The African Journal of Information Systems*, 8, 2, 86-113.

Rastogi, R., & Von Solms, R. (2012). Information security service branding - Beyond information security awareness. Systemics, *Cybernetics and Informatics*, 10, 6, 54-59.

Rotvold, G. M., & Braathen, S. J. (2008). Integrating security awareness into business and information systems education. *Journal of Business and Training Education*, 17, 8-15.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, 56, 70-82.

Ting, Y.-L. (2015). Tapping into students' digital literacy and designing negotiated learning to promote learner autonomy. *The Internet and Higher Education*, 26, 25-32.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2009). Aligning securiyty awareness with information systems security management. *Proceedings of the 4th Mediterranean Conference on Information Systems (MCIS)*, Paper 73. Turkey, Izmir.

Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating information security awareness: Research and practice gaps. *Information Security Journal*: A global perspective, 17, 5-6, 207-227.

Turney, C. S., Robinson, D., Lee, M., & Sourtar, A. (2009). Using technology to direct learning in higher education: The way forward. *Active Learning in Higher Education*, 10, 1, 71-83.