Towards information security savvy students in institutions of higher learning in Africa: A case of a university in Kenya

Conference Paper · May 2018

CITATIONS
0

READS
94

2 authors:

Joshua R A Ndiege
United States International University
12 PUBLICATIONS **16** CITATIONS
SEE PROFILE

Gabriel Otieno
KEMRI-Wellcome Trust Research Programme
8 PUBLICATIONS **101** CITATIONS
SEE PROFILE

IST-Africa 2018 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2018
ISBN: 978-1-905824-59-5

Towards Information Security Savvy Students in Institutions of Higher Learning in Africa: A Case of a University in Kenya

Joshua Rumo NDIEGE[1], Gabriel OKELLO[2]
School of Science and Technology
United States International University - Africa, Box 14634, Nairobi, 00800, Kenya
[1]*Tel: +254 0720727594, Email: jrumo@usiu.ac.ke*
[2]*Tel: +254 0722805371, Email: gokello@usiu.ac.ke*

Abstract: Whereas there is growing use of information technology (IT) within institutions of higher learning, little is known about the level of information security awareness (ISA) amongst students joining such institutions in developing countries and more specifically Africa. This study investigates ISA amongst undergraduate students in one of the universities within Nairobi in Kenya. From the study findings, it was clear that majority of the students did not possess adequate understanding of ISA. This was further affirmed by more than 60% of the students indicating not to have received any ISA training program before. We therefore submit that, there is a strong need to cultivate ISA culture amongst students joining institutions of higher learning. Cultivating this culture at the entry level will ensure that students as well as the institutions' communities at large have secure utilization of various IT resources. Furthermore, we recommend that ISA needs to be incorporated in the undergraduate curriculum to help enhance such awareness. Likewise, it would be valuable for such institutions to have ISA program as part of their wider information security strategy framework.

Keywords: Information Security Awareness, academic institution, university, Kenya.

1. Introduction

Considering the advances and the way 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 [1, 2, 3, 4, 5]. 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 [6, 7, 8, 9]. 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. It becomes sensible, therefore, to provide a learning environment that appreciates learners with this background. To this end, institutions of higher learning in both developed and developing countries continue to champion the use of IT within their institutions. 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 have been done on ISA within academia [10, 11, 12, 13, 7], the absence of studies which focus on students joining institutions of higher learning in developing countries and more specifically Africa is conspicuously lacking in information security literature. An attempt to bridge this gap by Adam and Rezgu [10] only focused on factors affecting ISA of end users in higher education in UAE. On the other hand, a study by Farooq, Isoaho, Virtanen, and Isoaho [12] looked at the correlation between individual factors and ISA amongst students in a university in Finland.

2. Objective

From the foregoing discussions, the specific objective of this study is to make a contribution to the 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.

3. Literature Review

Extant literature has indicated that information security awareness (ISA) is key in alleviating risks linked with information security breaches [14]. Line users' (immediate consumers of technology) naivety as well as unintentional behavior are viewed to be the most frequent causes of information security breaches [15, 16]. 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 institutions of higher learning 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 [12, 16]. 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 [17]. As a result, it has varied definitions within literature which translates into a lack of universal understanding of ISA. This may make it challenging for researchers to relate different studies on ISA. It is worth highlighting, that a number of literature in ISA fall short of explicitly defining the term [18, 19, 12]. 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 [20, 18, 21, 16, 22, 26, 27, 28]: **cognitive** (ISA is considered as one's state of mind defined by appreciation of the relevance of information security); **behavioural** (ISA is defined by information security behaviour like adherence to security policies) and **process** (processes or initiatives put in place by organizations to raise ISA).

IT continues to be a preferred choice as a tool for enhancing learning and teaching in the education sector [7, 4, 3]. And this is not only because institutions of higher learning 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.

In Kenya, institutions of higher learning continue to extend their programs to the internet and the need for virtual institutions continue to dominate their strategic directions and initiatives [29, 30]. This they do to help break geographical barriers and allow equitable access to education. Such increased usage 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 various programs offered in Kenyan universities reveals that information security education is mainly offered to those students who are enrolled in IT related degree programs [29]. 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.

Within institutions of higher learning, 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 such institutions, 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 take cognizance 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 [19, 32].

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' behaviour 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 behaviour that could compromise the IT resources within the institutions or make them vulnerable to threats and attacks.

4. Methodology

Positivist, quantitative research approach is employed in this study. The population of the study consisted all first year university students who had joined the university (380 students). A response rate of 82.9% (315 students returning completed questionnaires) was recorded. To ensure content validity, the questionnaire was reviewed by experts 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 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.

5. Results

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. 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. Those that were above 26 years comprised the smallest population at only 6.3%. With regard to the type of high school attended, of the sampled students, nearly two-thirds of the participants (61.0%) had attended private schools while 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 1); Information Security consisted of nine questions (see Table 2) and Physical Security comprised of three questions (see Table 3).

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. Interestingly, only 17.3% strongly agreed that they know how to protect against computer crime. A paltry 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 have such knowledge. 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.

Table 1: General Security Awareness

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

Source: The authors based on SPSS V22

On the theme of information security presented on Table 2, 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. Curiously, however, only 30.6% strongly agreed to be familiar with the appropriate methods for transmitting, storing, labelling and handling sensitive information. Merely 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.

Table 2: Information Security

Statements on the 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

Source: The authors based on SPSS V22

Regarding physical or resource security presented in Table 3, 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.

Table 3: Physical/Resource Security

Statements on 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	16	5.6	49	17.2	126	44.2	94	33.0

virus protection								
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

Source: The authors based on SPSS V22

6. Discussion

It is evident from the literature that issues related to information security awareness (ISA) has continued to draw attention not only from the scholars but also the practitioners [8, 12]. 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.

While 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 [19, 12]. This was confirmed in this study as 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 in Kenya have introduced computer studies [33].

In a summative evaluation of secondary schools, the Kenya Institute of Curriculum Development [34] observed that not only did the majority of schools have inadequate technological infrastructure, there was also limited integration of technology in pedagogy.

Students admitted in institutions of higher learning have heterogeneous background, 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.

Jansson and von Solms [35] 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 in Africa and other developing countries will be better prepared to deal with IT related threats.

As demonstrated in the literature [19, 12, 27], a number of studies continue to reveal that ISA remains one of the most effective methods of information security management. Consequently, cultivating such culture would go a long way in helping address information security challenges in educational institutions. 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.

7. Conclusions

Taken together, these results suggest that majority of the students joining institutions of higher learning do not 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 institutions of higher learning 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.

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.

Finally, this study appeals for more attention on comparative studies between developed economies like Europe and developing ones like Africa to understand similarities and differences regarding ISA and to set forth lessons than can be gleaned and learnt.

References

[1] K. Facer and R. Sandford, "The next 25 years? Future scenarios and future directions for education and technology," Journal of Computer Assisted Learning, vol. 26, no. 1, pp. 74-93, 2010.

[2] S. Manca and M. Ranierit, "Is facebook still a suitable technology-enhanced learning environment? An updated critical review of the literature from 2012-2015," Journal of Computer Assisted Technology, vol. 32, no. 6, pp. 503-528, 2016.

[3] M. M. Chingos, R. J. Griffiths, M. Christine and R. S. Richard, "Interactive online learning on campus: Comparing students outcomes in hybrid and traditional courses in the university system of Maryland," The Journal of Higher Education, vol. 88, no. 2, pp. 210-233, 2017.

[4] S. Assar, R. E. Amrani and R. T. Watson, "ICT and education: A critical role in human and social development," Information Technology for Development, vol. 16, no. 3, pp. 151-158, 2010.

[5] G. Akçayır, "Why do faculty members use or not use social networking sites for education?," Computers in Human Behavior, vol. 71, pp. 378-385, 2017.

[6] E. A. O. O'Connor and J. Domingo, "A practical guide, with theoretical underpinnings, for creating effective virtual reality learning environments," Journal of Educational Technology Systems, vol. 45, no. 3, pp. 343-364, 2017.

[7] F. AlTameemy, "Mobile phones for teaching and learning: Implementation and students' and teachers' attitudes," Journal of Educational Technology Systems, vol. 45, no. 3, pp. 436-451, 2017.

[8] T. L. Bailey and A. Brown, "Online student services: Current practices and recommendations for implementation," Journal of Educational Technology Systems, vol. 44, no. 4, pp. 450-462, 2016.

[9] C. S. M. Turney, D. Robinson, M. Lee and A. Sourtar, "Using technology to direct learning in higher education: The way forward," Active learning in higher education, vol. 10, no. 1, pp. 71-83, 2009.

[10] M. Adam and Y. Rezgu, "A comparative study of information security awareness in higher education based on the concept of design theorizing," in 2009 International Conference on Management and Service Science , Wuhan, China , 2009.

[11] L. Drevin, H. A. Kruger and T. Steyn, "Value-focused assessment of ICT security awareness in an academic environment," Computers & Security, vol. 26, no. 1, pp. 36-43, 2007.

[12] A. Farooq, J. Isoaho, S. Virtanen and J. Isoaho, "Information security awareness in educational institution: An analysis of students' individual factors," in 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Helsinki, Finland, 2015.

[13] A. Cox, S. Connolly and J. Currall, "Raising information security awareness in the academic setting," VINE, vol. 31, no. 2, pp. 11-16, 2001.

[14] N. S. Safa, R. Von Solms and S. Furnell, "Information security policy compliance model in organizations," Computers & Security, vol. 56, pp. 70-82, 2016.

[15] K. Parsons, E. Young, M. Butavicius, A. McCormac, M. Pattinson and C. Jerram, "The influence of organisational information security culture on cybersecurity decision making," Journal of Cognitive

Engineering and Decision Making: Special Issue on Cybersecurity Decision Making, vol. 9, no. 2, pp. 117-129, 2015.

[16] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius and M. Pattinson, "Individual differences and information security awareness,," Computers in Human Behavior, vol. 69, pp. 151-156, 2017.

[17] A. Tsohou, S. Kokolakis, M. Karyda and E. Kiountouzis, "Investigating information security awareness: Research and practice gaps," Information Security Journal: A global perspective, vol. 17, no. 5-6, pp. 207-227, 2008.

[18] C. Banerjee, A. Banerjee and P. D. Murarka, "An improvised software security awareness model," International Journal of Information, Communication and Computing Technology, vol. 1, no. 2, pp. 43-48, 2013.

[19] D. Budzak, "Information security – The people issue," Business Information Review, vol. 32, no. 2, p. 85–89, 2016.

[20] B. Bulgurcu, H. Cavusoglu and I. Benbasat, "Information Security Compliance: An empirical study of rationality-based beliefs and information security awareness," MIS Qauarterly, vol. 34, no. 3, pp. 523-527, 2010.

[21] J. D'Arcy, A. Hovav and D. Galletta, "User awareness of security countermeasures and its impact on information systems misuse: A deterrance approach," Information Systems Research, vol. 20, no. 1, pp. 79-98, 2009.

[22] T. Dinev, J. Goo, Q. Hu and K. Nam, "User behaviour towards protective information technologies: The role of national cultural differences," Information Systems Journal, vol. 19, no. 4, pp. 391-412, 2009.

[23] F. Hellqvist, S. Ibrahim, R. Jatko, A. Andersson and K. Hedström, "Getting their hands stuck in the cookie jar - Students' security awareness in 1:1 laptop schools," International Journal of Public Information Systems, vol. 2013, no. 1, pp. 1-19, 2013.

[24] G. M. Rotvold and S. J. Braathen, "Integrating security awareness into business and information systems education," Journal of Business and Training Education, vol. 17, pp. 8-15, 2008.

[25] A. Tsohou, M. Karyda, S. Kokolakis and E. Kiountouzis, "Aligning securiyty awareness with information systems security management," in Proceedings of the 4th Mediterranean Conference on Information Systems (MCIS), Turkey, Izmir, 2009.

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

[27] E. Kritzinger and E. Smith, "Information security management: An information security retrieval and awareness model for industry," Computer & Security, vol. 27, no. 5-6, pp. 224-231, 2008.

[28] R. Rastogi and R. von Solms, "Information security service branding - Beyond information security awareness," Systemics, Cybernetics and Informatics, vol. 10, no. 6, pp. 54-59, 2012.

[29] Commission for University Education, "News Updates," 20 September 2017. [Online]. Available: http://www.cue.or.ke/index.php/news-and-events.

[30] D. N. Mutisya and G. L. Makokha, "Challenges affecting adoption of e-learning in public universities in Kenya," E-Learning and Digital Media, vol. 13, no. 3-4, pp. 140-157, 2016.

[31] K. Parsons, A. McCormac, M. Pattinson, M. Butavicius and C. Jerram, "A study of information security awareness in Australian government organizations," Information Management & Computer Security, vol. 22, no. 4, pp. 334-345, 2014.

[32] C. Laybats and L. Tredinnick, "Information Security," Business Information Review, vol. 33, no. 2, pp. 76-80, 2016.

[33] Ministry of Education, "Digital Learning Program," 1 January 2016. [Online]. Available: http://www.education.go.ke/index.php/programmes/digital-learning-programme. [Accessed 22nd June 2017].

[34]Kenya Institute of Curriculum Development, "Home," 20 September 2017. [Online]. Available: http://kicd.ac.ke/93-departments/153-secondary-summative-evaluation.html.

[35] K. Jansson and R. von Solms, "Phishing for phishing awareness," Behaviour and Information Technology, vol. 36, no. 6, pp. 584-593, 2013.