Scientific Research Publishing

Journal of Computer and Communications, 2022, 10, 29-43
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Information Systems Security Threats and Vulnerabilities: A Case of the Institute of Accountancy Arusha (IAA)

Adam Aloyce Semlambo, Didas Malekia Mfoi, Yona Sangula

Department of Informatics, Institute of Accountancy Arusha (IAA), Arusha, Tanzania
Email: semlambo@gmaiil.com

How to cite this paper: Semlambo, A.A., Mfoi, M.D. and Sangula, Y. (2022) Information Systems Security Threats and Vulnerabilities: A Case of the Institute of Accountancy Arusha (IAA). *Journal of Computer and Communications*, **10**, 29-43.
https://doi.org/10.4236/jcc.2022.1011003

Received: September 13, 2022
Accepted: October 31, 2022
Published: November 3, 2022

Abstract

All modern computer users need to be concerned about information system security (individuals and organisations). Many businesses established various security structures to protect information system security from harmful occurrences by implementing security procedures, processes, policies, and information system security organisational structures to ensure data security. Despite all the precautions, information security remains a disaster in Tanzania's learning institutions. The fundamental issue appears to be a lack of awareness of crucial information security factors. Various companies have different security issues due to differences in ICT infrastructure, implementations, and usage. The study focuses on identifying information system security threats and vulnerabilities in public higher learning institutions in Tanzania, particularly the Institute of Accountancy Arusha (IAA). The study involved all employees of IAA, academics, and other supporting staff, which totalled 302, and the sample size was 170. The study utilised a descriptive research design, where the quantitative methodology was used through a five-point Likert scale questionnaire, and found that key factors that affect the security of information systems at IAA include human factors, policy-related issues, work environment and demographic factors. The study proposed regular awareness and training programs; an increase in women's awareness of information system security; proper policy creation and reviews every 4 years; promote actions that lessen information system security threats and vulnerabilities, and the creation of information system security policy documents independently from ICT policy.

Keywords

Information Systems, Information Security, Public Higher Learning Institutions, IAA

1. Introduction

Information security can be defined as the process of maintaining information confidentiality, integrity and availability against both internal and external vulnerabilities. Dependence on ICT infrastructure for daily use in achieving organisation objectives has made higher learning institutions a target of malicious activities from both within and from external factors [1]. Researchers have analysed different factors that contribute to poor Information System security in the learning environment. For example, the use of online learning facilities such as portals, online learning systems and mobile apps have increased security threats to learning environments [2] [3] [4]. Studies show that the number of internet users in Tanzania increased to 43.62 million just by 2018 [5]. This is about 45% of all adult citizens [6] and the majority of these users are from higher learning institutions with no proper knowledge on how to defend themselves/their institutions from hackers and online attacks. The threats to information system security have been reported to increase for both organisations and individuals [7]. The case is more alarming in learning environments of Tanzania as these incidences do not have formal ways of being documented, which are likely to reverse. Security attacks can result in loss of business, trust, reputation and money [8]. For example, researchers in reference [5] had their research showing the impact of cyber security attacks on learning environments in Tanzania. The study aims at identifying and categorising these threats and vulnerabilities and proposing appropriate solutions in the case of the learning environment of Tanzania.

There is a wealth of information on information system security around the world in the literature and international reports. According to Kaspersky's estimate, there were 445 million attacks in 2020 [9]. According to research in reference [10], 50% of Internet users admit to having experienced security breaches. According to research in reference [11], the typical data breach results in the loss of 25,575 records annually, costing an enterprise an estimated $3.92 million USD. Investors and customers may become less trusting of the impacted companies as a result of the data leak and stop doing business with them [12]. Collectively, it is clear that cyberattacks are on the rise [13]; as a result, it is important for stakeholders to remain aware of the variables affecting the security of information systems in learning environments.

As a result, studies about variables influencing information system security are provided in the literature. By concentrating on users' compliance with ICT policies, researchers in reference [14] analyse elements that affect the security of information systems. According to the report, disregarding ICT policies has a negative impact on the security of information systems. Reference [15] highlighted low adherence to the security culture as one of the causes of online vulnerability in a different study. The study in reference [16], in contrast, concentrated on the role of people in defending an organisation from attacks. In addition, references [17] and [18] hypothesised that variables including a lack of managerial backing,

a woefully inadequate information security policy, and a dearth of information security education programmes all play a role in the deficient security of corporate-owned information systems security. In this context, it is clear that there is no consensus on what influences information system security in the modern world. In order to identify the aspects affecting the security of information systems, this study does such analysis in public higher learning institutions in Tanzania, particularly the Institute of Accountancy Arusha (IAA).

There is evidence that the use of information systems is becoming more and more important to human activity, especially in learning environments like public higher learning institutions. Information systems are necessary for human activities and decision-making. The rising usage of computers and computer systems is due to the requirement for a reliable information system to fulfil consumer satisfaction [18]. In Tanzania, for example, ICT use is growing at a rate of 4.9 percent per year [19]. Currently, 60% of individuals worldwide are subscribers, compared to 50% of people in Tanzania who use the internet [10]. With this rise, it's clear that efficient use requires reliable information systems to improve the performance of the user organisation [18]. The study focuses on the efficient use of ICT infrastructures within the learning environment to eliminate information system security threats and vulnerabilities.

Evidently, safe supporting infrastructure and accompanying resources are necessary for information system reliability [2] [3] [20]. Nevertheless, according to reference [20] and [21], a number of factors influence the necessary level of online safety in eliminating information system security threats and vulnerabilities. These variables include administrative, technological, and human-related variables. Reference [22] asserts that more information system risks are being published online every day. Phishing, social engineering, supply chain attacks, zero-day and polymorphic attacks, IoT, and infrastructure attacks are a few of these dangers [23] [24]. This study aims to find out if these factors are the same for the higher learning environments in Tanzania.

Policies controlling the use of ICT provide the organisation with a solid administrative basis necessary to combat these challenges [25] [26]. This is why the current study assesses information system security threats and vulnerabilities in the learning environments.

2. Methodology

Through a descriptive design, the study employed a quantitative methodology. The 302 employees (both teaching and supporting staff) at IAA made up the study's population. Using the n = N/1 + N(e)2 formula proposed by Kothari [27], through a random sampling procedure, a sample of 170 participants was obtained at a 95% confidence level, 5% margin of error, and 50% population proportion from the population size of 302. Participants were instructed to select their thoughts by checking only one cell in the concept column on questionnaires that contained items ordered in the logical sequence of a 5-point Likert scale.

Passionately 1) strongly disagree, 2) disagree, 3) neither agree nor disagree, 4) agree, and 5) strongly agree. The validity and reliability of the data were ensured. Before distributing questionnaires, the participants' permission was taken into account. Additionally, questionnaires were forwarded to specialists for evaluation of their validity and reliability in relation to the goal of the study. A descriptive analysis was used in the study to analyse the information gathered through SPSS V26.

3. Findings and Discussions

This section concentrates its analysis of information system security threats and vulnerabilities on the Institute of Accountancy Arusha (IAA). The study was inspired by the fact that, like all other organisations, more and more security events affecting all kinds of businesses are being reported from the continent but very few within learning environments. The purpose of this study was to ascertain why information system security remains a concern for most learning institutions as well as for individual users. According to the research in reference [17], the elements affecting the security of information systems should be divided into a human, information security policy, work environment, and demographic aspects. Quantitative data were collected through questionnaires consisting of statements arranged in the logical order of a 5-point Likert scale, directing participants to choose their ideas by ticking only one cell in the concept column. 1) Strongly disagree, 2) disagree, 3) neither agree nor disagree, 4) agree, and 5) agree strongly.

Table 1. Determinants of information system security threats and vulnerabilities.

SN	Proposition	SDA %	DA %	NS %	A %	SA %
1) Human Factors						
1.1	It is a high-security risk to share personal credentials (user name and password) with anyone in the office or at the institute.	9.2	8.2	9.2	50.0	23.5
1.2	In our institution, information access is restricted accordingly by taking into account information that is public, protected, and restricted/secret.	21.4	35.0	14.0	29.6	6.1
1.3	We usually discuss office-related matters and share official documents on social networking sites such as WhatsApp groups.	2.0	20.4	20.6	24.3	32.7
1.4	I prefer to use my personal computer at work and connect to the institute network, as there are no restrictions on doing so.	9.2	17.3	12.2	28.0	33.3
1.5	I usually do notlock the screen or log out of my workstation while idle.	26.5	24.4	24.5	14.3	10.3
1.6	It is not important to have training on new ICT facilities before purchasing them as our experts (IT department) are competent with enough expertise to know everything.	2.0	20.4	20.6	24.3	32.7

Continued

1.7	**The institute has an ICT/information system security policy that is competent, known and followed by all employees.**	**21.4**	**29.6**	**13.3**	**29.6**	**6.1**
1.8	The institute always updates its ICT infrastructure (hardware and software) based on changes in technology.	2.4	20.7	20.3	24.6	32.0
1.9	The institute has a special sponsorship programme for information system security certifications and training.	46.4	20.6	12.3	10.7	10
2) Inadequate Information Security Policy						
SN	**Proposition**	**SDA**	**DA**	**NS**	**A**	**SA**
2.1	The institute provides regular awareness and training programmes about ICT and information system security policies.	39.0	31.4	24.6	5.0	0.0
2.2	Our institute has an ICT/information system security policy that was created by involving all the stakeholders and is known to all employees of the institute.	15.3	17.7	50.4	16.6	0.0
2.3	The institute, in collaboration with the IT department, follows all the appropriate guidelines in implementing ICT/Information system security policies for proper utilisation of ICT facilities.	23.3	21.4	34.4	11.7	9.2
3) Work Environment						
SN	**Proposition**	**SDA**	**DA**	**NS**	**A**	**SA**
3.1	Management inspires information system security training and awareness programmes for all employees.	28.6	29.6	13.3	25.5	3.0
3.2	The institute's information system security culture is well established, as every employee is aware of all the concerning habits in the use of ICT infrastructures that can lead to information system security threats and vulnerabilities.	23.3	26.3	21.4	26.7	2.3
3.3	There are restrictions on the use of optimisation software to simplify work for individual best performance and deadlines in completing daily office objectives.	24.3	20.4	39.0	10.6	5.7
3.4	The institute provides guidelines on the appropriate use of the Internet through policies such as accessing dubious websites, accessing the institute website on a public network, and opening emails from unknown senders.	20.3	21.7	31.8	16.8	9.4
3.5	IAA categorises information access as public, protected, or restricted (secret) and assigns credentials accordingly.	20.4	25.3	15.4	18.6	20.1
4) Demographic Variables						
4.1	Information system security is more of a technical issue; thus it is a male field than a female one.	22.6	26.4	20.9	20.7	9.4
4.2	Being at IAA for many years has helped me to develop skills and knowledge in information system security policies, rules, and guidelines to protect both myself and the institute. The same cannot be said for new employees.	26.7	28.3	30.1	8.2	6.7

Continued

4.3	**I believe that young people are more teachable about new technologies and safety precautions than senior institute employees.**	**11.2**	**13.7**	**17.2**	**30.6**	**27.3**
4.4	The Internet use habits of junior employees attract more information system security risks and vulnerabilities to the institute compared to senior employees.	9.2	10.6	25.9	27.4	26.9
4.5	I believe that employees with appropriate knowledge and training on the Internet, cybersecurity and information system security training can protect the institute against information system security threats and vulnerabilities from both internal and external IAA.	12.9	13.4	15.8	27.4	30.5

Source: Researchers (2022).

3.1. Human Factor

Reference [16] takes into account human variables, including how people behave physically and psychologically in connection to information system security. Additionally, the study in reference [28] noted that the suitability of user behaviours when using the system is crucial to an organisation's information system security success. This area of human variables includes carelessness, lack of skills, and trust. Details on the information in **Table 1** are provided in the next section.

Trust: According to this study, trust is the human component having the greatest impact on the security of information systems. Because of recommendations from co-workers or personal experience, one comes to trust another individual [29]. Although trust seems admirable, if safety measures are not implemented, it can turn into a point of attack [30]. Employees exchanging login information or data without taking security into account are one of the dangerous behaviours related to trust [31] [32]. These actions exacerbate the risks to information system security [33]. Though findings show that about 73.5% of respondents know the risk of sharing personal credentials, there is still a small number of people who do not understand this risk, which can result in catastrophic information system security risks and vulnerabilities at the institute. The same applies to the restriction of information based on public, protected, and restricted (secret) (Item 1.2).

Carelessness: According to reports, human carelessness also has an impact on the security of information systems in a learning environment. Carelessness is defined as an individual's activity or behaviour that deliberately or unknowingly jeopardises the information system's security. For instance, discussing work-related matters in emails or on public networks, where it is estimated that the average email user sends up to 112 emails per day and that about one in every seven of these emails is connected to office gossip [34]. Social media chitchat about work-related issues can be irresponsible and reveal confidential information to unwanted or unauthorised parties, increasing security risks and vulnerabilities for a firm. Results showed that more than half of respondents (Item 1.3) agreed to

discuss office-related issues on social media, which results in numerous information system security threats and vulnerabilities. Additionally, additional actions like allowing a visitor to use a company computer or connecting a personal computer to the network without taking the proper security procedures raise alarms about security (Item 1.4). Security hazards can also be brought about by leaving workplace computers unattended (Item 1.5), introducing new hardware or software to users without proper training (Item 1.6), and operating ICT infrastructures without an ICT/IS security policy (Item 1.7). Additionally, employing old technology and software, among many other negligent practices (Item 1.8), is thought to put corporate information security at risk.

Lack of skills: Table 1 found a further human element affecting information security in a learning environment, namely a lack of skills. According to research by in reference [35], many people lack faith in the information system security expertise and experience of their specialists to handle current security concerns. Due to the high cost of most information security certifications for individuals (Item 1.9), this is a challenge. Additionally, the majority of businesses are reluctant to sponsor their staff members for professional qualifications [36]. On the other hand, as demonstrated the study in reference [37], common users also lack capabilities. This combination eventually has an impact on initiatives to protect the security of information systems.

3.2. Inadequate Information Systems Security Policies

An organisation's personnel's duties and responsibilities for safeguarding its information systems are specified in its information security policy [38]. Policies ensure proper administration of technology resources if they are followed [39]. If not addressed properly, this group of factors can lead to information system security threats and vulnerabilities, as explained in the following subsections.

Lack of Information System Security Policy Training: The most prevalent component within the policy category is a lack of information security policy training. Users would receive training to equip them with the necessary knowledge to ensure information system security [25] [40]. Users who go through training are given reliable tools and the know-how to keep company information secure. Table 1 shows that most of the people who answered the survey at IAA did not get any training on ICT or information system security policies (Item 2.1). This means that they use ICT facilities without knowing the right rules and safety features to protect themselves and their institution.

Poor Creation of Information System Security Policies: one of the information system security threats and vulnerabilities cause is the poor creation of information system security policy. Findings of this study show that participants were unaware of such policies, which means they were not involved in their creation as stakeholders (Item 2.2). Studies in reference [13] provide guidelines to adhere to and minimum standards for a security policy. Data security, Internet and network services governance, use of company-owned devices, physical secu-

rity, incident handling and recovery, monitoring and compliance, and policy administration are the parts of the security policy that they advise including. In addition to these requirements, reference [25] stressed how important it was to include all security stakeholders in the process of writing the policy. They will be able to share their expertise, thoughts, and ideas because the organisation's weak spots will be exposed [41]. A good policy will be made if you make sure to include important stakeholders and follow the standards that are suggested.

Poor Implementation of Information Systems Security Policies: Poor information systems security policy application, as shown in **Table 1**, is one of the variables that without proper addressing, can lead to information system security threats and vulnerabilities in an organisation (item 2.3). According to the study in reference [42], policy implementation challenges arise because the majority of policies are created for compliance reasons rather than to address actual security requirements. Also, say that when information systems policies aren't put into place properly, they become useless documents that make the system more vulnerable. With the right implementation of information system security policies [20], the company could find implementation issues, limitations, and technological changes that need to be taken into account when making policies.

3.3. Work Environment

This definition is adapted from refence [43] and [44] and refers to the social elements and physical circumstances in which users of information systems carry out their work. The category of elements most frequently identified to have an impact on the security of information systems in the workplace is Individual factors of this sub-category are detailed in the next sub-section according to **Table 1**.

Inadequate Management Support: inadequate management support for information system security in an organisation can lead to security threats and vulnerabilities. Findings show that IAA management does not provide awareness and training in information system security policies to employees (item 3.1). Senior managers should serve as role models for the organisation by ensuring appropriate training and awareness campaigns, as well as by positively influencing their security behaviour [15] [45]. Other strategies used by management to assist subordinates include idealising security impact inside an organisation, giving each person special consideration, and inspiring drive [46]. According to researchers in reference [47] and [48], management's failure to support security programmes increases the organisation's information system security risk and vulnerabilities.

Organizational Security Culture: Another issue that is frequently mentioned in relation to information system security is organisational security culture. Establishing policies, norms, and guidelines that direct employees' behaviour within a company becomes part of the organisation's culture [16]. The organisation's inability to establish the proper security culture has led to a rise in security threats associated with information systems [15] [33]. Themanagement must es-

tablish the proper security culture and integrate it into the long-term agenda. Sadly, research indicates that IAA does not operate in this way (Item 3.2).

Workload: Another aspect included in the work environment category that has been noted is workload. The workload in this essay refers to the volume of work that must be finished within the allotted time and resources [49]. Findings show that there are no restrictions on the use of optimisation software at IAA, which can lead to information system security threats and vulnerabilities. According to studies, employees' ambition to optimise production with limited resources leads to a number of information system security threats and vulnerabilities. Over time, the organisation's pressure on workers to meet higher financial targets raises the possibility that they will violate security [50]. Because of the constant pressure to stretch resources, employees put performance over security concerns [51].

Internet and Network Use: This describes how much a company relies on the Internet and networks to run its operations. The need for an Internet connection in the current business climate is essential to being competitive [7] [52]. The usage of the Internet becomes a risk to the security of information systems if the organisation uses it to support its operations without properly weighing the security concerns [53]. Findings show that respondents are unaware of any restrictions regarding the use of internet and network facilities at IAA (Item 3.4). This can result in the inappropriate use of such services, which leads to information system security risks and vulnerabilities.

Access Control: As users demand greater privileges when interacting with the system, access controls typically become less effective [54]. Instead of just making someone happy at the expense of overall security, the company must regulate system accessibility based on an individual's tasks and responsibilities [55]. The information must be classified into three types: public, protected, and restricted. A system is vulnerable to threats if system access policies are not defined [56]. Respondents of the study have mixed feelings on the exitance of such controls at IAA (Item 3.5).

3.4. Demographic Variables

This section presents information on a variety of demographic variables that have been implicated in information system security threats and vulnerabilities. Gender, age, level of education, experience, and managerial function, according to reference [57], can all be used to predict a person's intention to adhere to information system security as described below.

Gender: According to this study, gender can lead to various information system security threats and vulnerabilities. Findings show that it is the perception of the majority of respondents that information system security is more likely to be a male practice than a female one (Item 4.1). This perception leaves behind the majority of female employees, who are competent enough and can bring the required change in securing the organisations' information systems. Researcher

in reference [58] found that females are more likely than males to perceive high levels of security threats. In a different study, reference [20] found that men are more likely than women to exhibit superior information security behaviours. Researchers in reference [36] say that since information system is thought of as a male-dominated field, it is important to get more women to sign up for information systems security courses and get them interested in a career in information system security.

Work Experience: The presumption is that an individual's employment history, both technical and non-technical, has some bearing on how appropriate their information security behaviour is. According to reference [59], experienced staff are safer thanks to their prior exposure to handling various security events. Additionally, work experience offers the chance for training, which imparts important knowledge for defence against assaults [56]. According to the findings of this study, experience in a less secure environment cannot provide an employee with security knowledge and experience (item 4.2). As explained in previous subcategories, without an adequate information system security training and awareness program, it is likely for the institute to have vulnerabilities and threats in its information systems.

Internet User Age: These study findings show that the internet use habits of young people have more information system security incidents compared to senior employees (items 4.3 and 4.4). According to the researcher in reference [60], younger individuals are more likely than older people to be aware of information system security threats and vulnerabilities. They are similarly irresponsible with their security knowledge [61]. Additionally, when undergoing new changes, youthful people are simple to teach, which is important when the firm changes its security procedures [60]. Based on these results, more work needs to be done to deal with how careless young people are and to teach adults more about security vulnerabilities and threats at IAA.

Level of Education: The results of this study show that the people who took part in it think that a level of education in the internet, cyber security, and information system security can protect the institute from vulnerabilities and threats to information system security (Item 4.5). According to research in reference [62], businesses face a variety of information security risks as a result of the information being shared via the Internet. These difficulties with maintaining information integrity and confidentiality depend on the understanding, education, and conduct of the end user. A trained cyber-literate workforce and an education system that can create such a workforce are necessary for successfully defending the organisation's vital infrastructure against cyberattacks [63].

4. Conclusion and Recommendations

The Institute of Accountancy Arusha (IAA) was used as a case study to understand the main factors that contribute to the information system security threats and vulnerabilities in a learning environment. This research put information sys-

tem security threats and vulnerabilities into four groups. The first category comprises human elements, including carelessness, level of skill, and trust. The inadequacy of information security policies, which includes problems with policy creation, implementation, and a lack of security training, was the second category. The study also looked at the "work environment", which includes things like support from management, organisational security culture, workload, Internet and network use, and access control. Last but not least, the study included variables related to gender, age, education level, and work experience under the category of "demographic variables". The study findings showed that almost all these categories received negative responses and contributed highly to the information system risk and vulnerabilities at the institute. Moreover, there is an unregulated level of trust, negligence, and inadequate security measures. According to these results, the study suggests that:

1) Organisations should regularly train their staff to improve their information system security proficiency.

2) Given that women are disproportionately affected, the institutes should make a concerted effort to increase their awareness.

3) The institute should create up-to-date policies that fully handle the issues with contemporary information system security and update in a minimum of every four (4) years.

4) The institute ought to promote actions that lessen exposure to information system security concerns.

5) The institute should consider creating an independent information system security policy document as currently, information system security policy is just a section within ICT policy which hinder its adequacy and relevance.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Kundy, E.D. and Lyimo, B.J. (2019) Cyber Security Threats in Higher Learning Institutions in Tanzania A Case Study of University of Arusha and Tumaini University Makumira. *Olva Academy—School of Researchers*, **2**, 1-37.

[2] Semlambo, A., Almasi, K. and Liechuka, Y. (2022) Perceived Usefulness and Ease of Use of Online Examination System: A Case of Institute of Accountancy Arusha. *International Journal of Scientific Research and Management* (*IJSRM*), **10**, 851-861. https://doi.org/10.18535/ijsrm/v10i4.ec08

[3] Semlambo, A., Almasi, K. and Liechuka, Y. (2022) Facilitators' Perceptions on Online Assessment in Public Higher Learning Institutions in Tanzania: A Case Study of the Institute of Accountancy Arusha (IAA). *International Journal of Scientific Research and Management* (*IJSRM*), **10**, 34-42. https://doi.org/10.18535/ijsrm/v10i6.lis02

[4] Lubua, E.W., Semlambo, A. and Pretorius, P.D. (2017) Factors Affecting The Use of Social Media in the Learning Process. *South African Journal of Information Man-*

agement, **19**, a764. https://doi.org/10.4102/sajim.v19i1.764

[5] Nfuka, E.N., Sanga, C. and Mshangi, M. (2015) The Rapid Growth of Cybercrimes Affecting Information Systems in the Global: Is this a Myth or Reality in Tanzania? *International Journal of Information Security Science*, **3**, 182-199.

[6] Tanzania Communication Regulatory Authority. (2022) 2022 Quarterly Statistics Reports. Tanzania Communication Regulatory Authority, Dar es Salaam.

[7] Saunders, J. (2017) Tackling Cybercrime—The UK Response. *Journal of Cyber Policy*, **2**, 4-15. https://doi.org/10.1080/23738871.2017.1293117

[8] Lewis, J. (2018) Economic Impact of Cybercrimes-No Slowing Down. McAfee, Santa Clara. https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf

[9] Kaspersky (2021) Top Ransomware Attacks of 2020. Kaspersky, Moscow.

[10] International Telecommunication Union (2021) Cyber Security in Tanzania: Country Report. International Telecommunication Union, Geneva.

[11] International Business Machine Cooperation (IBM) (2021) Cost of Data Breach Report. International Business Machine Cooperation, Armonk.

[12] Gordon, L.A., Loeb, M.P. and Zhou, L. (2011) The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs? *Journal of Computer Security*, **19**, 33-56. https://doi.org/10.3233/JCS-2009-0398

[13] Lubua, E.W. and Pretorius, P.D. (2019) Ranking Cybercrimes Based on Their Impact on Organisations' Welfare. 2019 *THREAT Conference Proceedings*, Johannesburg, 26-27 June 2019, 1-11.

[14] Al-Omari, A., El-Gayar, O. and Deokar, A. (2012) Security Policy Compliance: User Acceptance Perspective. 2012 45*th Hawaii International Conference on System Sciences*, Maui, 4-7 January 2012, 1-10. https://doi.org/10.1109/HICSS.2012.516

[15] AlHogail, A. (2015) Design and Validation of Information Security Culture Framework. *Computers in Human Behavior*, **49**, 567-575. https://doi.org/10.1016/j.chb.2015.03.054

[16] Alhogail, A., Mirza, A. and Bakry, S.H. (2015) A Comprehensive Human Factor Framework for Information Security in Organisations. *Journal of Theoretical and Applied Information Technology*, **78**, 201-211.

[17] Arbanas, K. and Hrustek, N.Ž. (2019) Key Success Factors of Information Systems Security. *Key Success Factors of Information Systems Security*, **43**, 131-144. https://doi.org/10.31341/jios.43.2.1

[18] Almazán, D.A., Tovar, Y.S. and Quintero, J.M. (2017) Influence of Information Systems on Organisational Results. *Contaduría y Administración*, **62**, 321-338. https://doi.org/10.1016/j.cya.2017.03.001

[19] Tanzania Communication Regulatory Authority (TCRA). (2022) Communication Statistics Quarter 2 2021/2022. Tanzania Communication Regulatory Authority, Dar es Salaam.

[20] Alotaibi, M., Furnell, S. and Clarke, N.L. (2016) Information Security Policies: A Review of Challenges and Influencing Factors. 2016 11*th International Conference for Internet Technology and Secured Transactions*, Barcelona, 5-7 December 2016, 352-358. https://doi.org/10.1109/ICITST.2016.7856729

[21] Assefa, T. and Tensaye, A. (2021) Factors Influencing Information Security Compliance: An Institutional Perspective. *SINET*: *Ethiopian Journal of Science*, **44**, 108-118. https://doi.org/10.4314/sinet.v44i1.10

[22] Williams, S. (2021) Cyberattacks on Organisations Worldwide Surge 40% in 2021. Security Brief, New Zealand.

[23] Broadhurst, R.G., Skinner, K., Sifniotis, N., Matamoros-Macias, B. and Ipsen, Y. (2018) Phishing and Cybercrime Risks in a University Student Community. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3176319

[24] Lohani, S. (2019) Social Engineering: Hacking into Humans. *International Journal of Advanced Studies of Scientific Research*, **4**, 385-395.

[25] Alqahtani, F.H. (2017) Developing an Information Security Policy: A Case Study Approach. *Procedia Computer Science*, **124**, 691-697. https://doi.org/10.1016/j.procs.2017.12.206

[26] ISO/IEC 27000:2018. (2018) Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary. International Organization for Standardization.

[27] Kothar (2004) Research Methodology; Methods and Techniques. New Age International Publishers, New Delhi.

[28] Glaspie, H.W. and Karwowski, W. (2018) Human Factors in Information Security Culture: A Literature Review. *Proceedings of the AHFE* 2017 *International Conference on Human Factors in Cybersecurity*, Los Angeles, 17-21 July 2017, 269-281. https://doi.org/10.1007/978-3-319-60585-2_25

[29] Rajaonah, B. (2017) A View of Trust and Information System Security under the Perspective of Critical. *Revue des Sciences et Technologies de l'Information—Série ISI: Ingénierie*, **22**, 109-133.

[30] Sapronov, K. (2020) The Human Factor and Information Security. Kaspersky, Moscow.

[31] Astakhova, L.V. (2016) The Ontological Status of Trust in Information Security. *Scientific and Technical Information Processing*, **43**, 58-65. https://doi.org/10.3103/S0147688216010123

[32] Robinson, S.C. (2019) Factors Predicting Attitude toward Disclosing Personal Data Online. *Journal of Organizational Computing and Electronic Commerce*, **28**, 214-233. https://doi.org/10.1080/10919392.2018.1482601

[33] Brock, V. and Khan, H.U. (2017) Big Data Analytics: Does Organizational Factor Matters Impact Technology Acceptance? *Journal of Big Data*, **4**, Article No. 21. https://doi.org/10.1186/s40537-017-0081-8

[34] Mitra, T. and Gilbert, E. (2012) Have You Heard? How Gossip Flows Through Workplace Email. *Proceedings of the* 6*th International AAAI Conference on Weblogs and Social Media*, Dublin, 4-7 June 2012, 242-249.

[35] Kagwiria, C. (2020) Cyber Security Skills Gap in Africa. African Advanced Level Telecommunications Institute, Nairobi.

[36] Patrick, H., Niekerk, B.V. and Fields, Z. (2018) Information Security Management: A South African Public Sector Perspective. In: Fields, Z., Ed., *Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution*, IGI Global, Hershey, 382-405. https://doi.org/10.4018/978-1-5225-4763-1.ch014

[37] Cisco (2016) Mitigating the Cybersecurity Skills Shortage. Cisco, San Francisco.

[38] Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010) Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, **34**, 523-548. https://doi.org/10.2307/25750690

[39] Watters, P.A. and Ziegler, J. (2016) Controlling Information Behaviour: The Case for Access Control. *Behaviour & Information Technology*, **35**, 268-276.

https://doi.org/10.1080/0144929X.2015.1128976

[40] Ghazvini, A. and Shukur, Z. (2016) Awareness Training Transfer and Information Security Content Development for Healthcare Industry. *International Journal of Advanced Computer Science and Applications*, **7**, 361-370. https://doi.org/10.14569/IJACSA.2016.070549

[41] Hina, S. and Dominic, P.D. (2018) Information Security Policies' Compliance: a Perspective for Higher Education Institutions. *Journal of Computer Information Systems*, **60**, 201-211. https://doi.org/10.1080/08874417.2018.1432996

[42] Lopes, I. and Oliveira, P. (2015) Implementation of Information Systems Security Policies: A Survey in Small and Medium Sized Enterprises. In: Rocha, A., Correia, A., Costanzo, S. and Reis, L., Eds., *New Contributions in Information Systems and Technologies*, Springer International Publishing, Bragança, 459-468. https://doi.org/10.1007/978-3-319-16486-1_45

[43] Greene, G. (2010) Assessing the Impact of Security Culture and the Employee-Organization Relationship on IS Security Compliance I. 5*th Annual Symposium on Information Assurance*, Albany, 16-17 June 2010, 1-8.

[44] Humaidi, N. and Balakrishnan, V. (2015) The Moderating Effect of Working Experience on Health Information System Security Policies Compliance Behaviour. *Malaysian Journal of Computer Science*, **28**, 70-92.

[45] Kearney, W.D. and Kruger, H.A. (2016) Can Perceptual Differences Account for Enigmatic Information Security Behaviour in an Organisation? *Computers & Security*, **61**, 46-58. https://doi.org/10.1016/j.cose.2016.05.006

[46] Choi, M. (2016) The leadership of the Information Security Manager on the Effectiveness of Information Systems Security for Secure Sustainable Computing. *Sustainability*, **8**, 638-648. https://doi.org/10.3390/su8070638

[47] Padayachee, K. (2012) Taxonomy of Compliant Information Security Behavior. *Computers & Security*, **31**, 673-680. https://doi.org/10.1016/j.cose.2012.04.004

[48] Dotto, M.H. (2015) Effectiveness of the Electronic Records Management System in the Selected Courts of Tanzania. Collage of Business Education (CBE), Dar es Salaam.

[49] Vernon-Bido, D., Grigoryan, G., Kavak, H. and Padilla, J. (2018) Assessing the Impact of Cyberloafing on Cyber Risk. *Proceedings of the Annual Simulation Symposium*, Baltimore, 15-18 April 2018, Article No. 11.

[50] Martin, N., Rice, J. and Martin, R. (2016) Expectations of Privacy and Trust: Examining the Views of IT Professionals. *Behaviour & Information Technology*, **35**, 500-510. https://doi.org/10.1080/0144929X.2015.1066444

[51] Amraoui, S., Elmaallam, M., Bensaid, H. and Kriouile, A. (2019) Information Systems Risk Management: Litterature Review. *Computer and Information Science*, **12**, 1-20. https://doi.org/10.5539/cis.v12n3p1

[52] Khan, H.U. and AlShare, K.A. (2019) Violators Versus Non-Violators of Information Security Measures in Organisations—A Study of Distinguishing Factors. *Journal of Organisation Computing and Electronic Commerce*, **29**, 4-23. https://doi.org/10.1080/10919392.2019.1552743

[53] Tawalbeh, L., Muheidat, F., Tawalbeh, M. and Quwaider, M. (2020) IoT Privacy and Security: Challenges and Solutions. *Applied Sciences*, **10**, Article No. 4102. https://doi.org/10.3390/app10124102

[54] Sindiren, E. and Ciylan, B. (2018) Privileged Account Management Approach for Preventing Insider Attacks. *International Journal of Computer Science and Network*

Security, **18**, 33-42.

[55] Pesic, D. and Veinović, M.Đ. (2016) Privileged Identities—Threat to Network and Data Security. *International Scientific Conference on ICT and E-Business Related Research*, Belgrade, 22 April 2016, 154-160. https://doi.org/10.15308/Sinteza-2016-154-160

[56] Connolly, L., Lang, M. and Tygar, D. (2014) Managing Employee Security Behaviour in Organisations: The Role of Cultural Factors and Individual Values. 2014 *International Federation for Information Processing*, Marrakech, 2-4 June 2014, 417-430. https://doi.org/10.1007/978-3-642-55415-5_35

[57] Barlow, J., Warkentin, M., Ormond, D.K. and Dennis, A.R. (2018) Don't Even Think About It! The Effects of Antineutralization, Informational, and Normative Communication on Information Security Compliance. *Journal of the Association for Information Systems*, **19**, 689-715. https://doi.org/10.17705/1jais.00506

[58] McGill, T. and Thompson, N. (2018) Gender Differences in Information Security Perceptions and Behaviour. *Australasian Conference on Information Systems* 2018, Sydney, 3-5 December 2018, 1-10. https://doi.org/10.5130/acis2018.co

[59] Erceg, A. (2019) Information Security: Threat from Employees. *Tehnički Glasnik*, **13**, 123-128. https://doi.org/10.31803/tg-20180717222848

[60] Fatokun, F.B., Hamid1, S., Norman, A. and Fatokun, J.O. (2019) The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: *An Empirical Investigation on Malaysian Universities*. *Journal of Physics*: *Conference Series*, **1339**, Article ID: 012098. https://doi.org/10.1088/1742-6596/1339/1/012098

[61] Levesque, F.L., Fernandez, J.M. and Batchelder, D. (2017) Age and Gender as Independent Risk Factors for Malware Victimisation. *Proceedings of the* 31*st British Computer Society Human Computer Interaction Conference*, Sunderland, 3-6 July 2017, Article No. 46. https://doi.org/10.14236/ewic/HCI2017.48

[62] Bostan, A. (2015) Impact of Education on Security Practices in ICT. *Tehnicki Vjesnik*, **22**, 161-168. https://doi.org/10.17559/TV-20140403122930

[63] Catota, F.E., Morgan1, G. and Sicker, D.C. (2019) Cybersecurity Education in a Developing Nation: The Ecuadorian Environment. *Journal of Cyber Security*, **5**, tyz001. https://doi.org/10.1093/cybsec/tyz001