University of Dar es Salaam Library Journal
Vol 17, No 2 (2022), pp 94-114
ISSN: 0856-1818

Factors Affecting the Security of Information Systems in Africa: A Literature Review

Edison Wazoel Lubua
Institute of Accountancy Arusha, Tanzania
Email: edison.lubua@iaa.ac.tz

Adam Aloyce Semlambo
The Open University of Tanzania, Tanzania
Email: semlambo@gmail.com

Catherine G Mkude
The Open University of Tanzania, Tanzania
Email: catherine.mkude@out.ac.tz

Abstract

This study determined factors affecting the security of Information Systems in Africa. Also, it established the quality of publications in the area of Information Security. The study is based on peer-reviewed publications conducted in Africa. The study adopted the mixed research approach. The study used a systematic literature review, with part of the analysis using descriptive analysis. In total, 70 papers formed the population of publications extracted in the area of Information Security. In addition, 37 papers had the quality to be included in the analysis of factors affecting Information Security. The study found that information Security factors are in four key categories: human factors, policy-related issues, work environment, and demographic factors. Overall, the work environment is the most reported category affecting the security of Information Systems in Africa. In addition, gender is the highest reported individual factor associated with the insecurity of Information Systems; female is the highly affected gender. Other factors include the lack of Information Security training, the unchecked level of trust, carelessness and poor security policies. The study recommends training programs, policy improvement and promoting behaviours that minimise exposure to attacks.

Keywords: Information systems, information security, information systems security, Africa
https://dx.doi.org/10.4314/udslj.v17i2.7

Introduction

Information Security is the state of being protected against the unauthorised use of information, electronic data, software applications and hardware (Lundgren & Möller, 2017). The main goal of Information Security is to achieve information confidentiality, integrity and availability (Lundgren & Möller, 2017). In a case where the security of Information Systems is compromised, the organisation faces risks such as information breaches, data loss, cyber-attacks and even the loss of business (Thorwat, 2018; Al-Omari, El-Gayar, & Deokar, 2012; Arbanas & Hrustek, 2019). It is estimated that the loss of resources due to poor Information Security will cost the world about US$ 10.5 trillion by 2025 (Sausalito, 2020). This loss is greater than the GDP (Nominal) earned in Africa, which is 2.49 Trillion US$ (International Monetary Fund, 2021). Therefore, it is indisputable that resources that could be used to enrich the standard of living of people are wasted through criminal schemes due to inadequate electronic protection.

The literature and international reports present a vast amount of data on Information Security around the world. Kaspersky has recently reported that 445 million attacks were detected in 2020 (Kaspersky, 2020). A study by the International Telecommunication Union (ITU) (2020) reports that 50% of Internet users acknowledge being victims of security breaches. The cost of a data breach to an organisation is estimated to be 3.92 million US dollars, with an average data breach of 25,575 records per year, as reported by the International Business Machine Cooperation (IBM) (2020) and the Global Cybersecurity Index (2017). This data breach deteriorates trust and lead investors and customers to refrain from doing business with affected organisations (Gordon, Loeb, & Zhou, 2011). Collectively, it is evident that cyber-attacks are ever-increasing (Lubua & Pretorius, 2019); therefore, the knowledge of factors affecting the security of Information System remains significant among the stakeholders.

Accordingly, the literature provides studies on factors that affect Information System Security. Al-Omari, El-Gayar and Deokar (2012) analyse factors that affect the security of Information Systems by focusing on users' compliance with Information and Communication Technology (ICT) policies. The study asserted that the failure to comply with ICT policies negatively affects the security of Information Systems. In another study, Alhogail (2015) emphasised poor adherence to the security culture as one of the reasons for online insecurity. Meanwhile, the study by Alhogail, Mirza and Bakry (2015) focused on human factors in protecting an organisation against attacks. In addition, Arbanas and Hrustek (2019) suggested factors such as the lack of management support, inadequate Information Security policy, and the lack of Information Security education programs, to contribute to the poor security of Information Systems owned by corporations. With this background, it is evident that there is no common position on factors affecting the security of Information Systems in a contemporary environment. This study is motivated by the lack of a common point of reference on factors affecting the security of information systems in Africa. Therefore, the study develops a common point of reference to studies of this nature. Also, the study established the quality of publications in the area of Information security.

Information Security Attributes Within an Organisation

In the past, it was easy to verify an organisation's security through physical audits and related checks (Ana-Maria, Bîzoi, & Filip, 2010). Today, verification is difficult because businesses largely depend on integrated systems connecting many stakeholders (Manaseer & Alawneh, 2019). The publication by Mir, Mohammad and Quadri (2016) and Popescul (2011) recommended the level of confidentiality, integrity and availability to form attributes for a secure Information System within the organisation. The position of this study is supported by Zoto et al (2018) and Sapronov (2020). In this document, the study adopts these attributes and will explain them in the next part. The attributes are information confidentiality, data integrity and system availability.

Information confidentiality ensures that data (or information) are only accessible to authorised individuals (Bulgurcu, Cavusoglu, & Benbasat, 2010). However, even within the organisation, a piece of information may not be accessible to everyone. This is the reason why Alhogail, Mirza and Bakry (2015) suggested protecting the information from unfaithful employees since they are linked to most attacks within the organisation. In addition, the study by Kaspersky (2020) suggests that there are 4000 attacks released every day by hackers. In order to ensure the protection of Information Systems from attacks, the study by Mir, Mohammad and Quadri (2016) emphasises the use of encryption for stored data and data in transit. The use of two-factor authentications, biometrics, and asymmetry encryption is recommended to ensure that only those authenticated access the system (Al-Omari, El-Gayar, & Deokar, 2012).

Integrity refers to data accuracy and completeness; it aims to protect data from being misused or modified by unauthorised parts (Dieser, Covella, & Olsina, 2014). According to Limaye (2013), protecting data from unauthorised access is the first step in preventing unintended data modification. In addition, the protection takes care of data that are in storage or transit. This is possible by ensuring the right access to the system for each user, based on their roles and the need for data within the organisation (Watters & Ziegler, 2016). Other factors that can affect data integrity include employees' unguided behaviours, the absence of a competent ICT department responsible for security management, the lack of senior management support, insufficient technical equipment, and technological faults (hardware/software) (Patrick, Niekerk, & Fields, 2018). In addition, Bolek et al (2016) suggested factors such as insufficient software and the absence of internal guidelines and standards. Furthermore, other factors, such as the lack of financial resources, technological progress, and natural disasters, affect the level of data integrity equally.

System availability is associated with the accessibility of data and information to authorised users (Dieser, Covella, & Olsina, 2014). In the study by Bolek, Látečková, Romanová, and Korcek (2016), this aspect of Information Systems security is linked to both external and internal factors. The following are common factors affecting information availability: human activities, environmental factors and technological factors (Cvitić, Perakovic & Kuljanić, 2017). In addition, the study by Ramadhani, Sam and Kalegele (2017) identifies factors such as power outages, installation of access points, network subscription, the knowledge of the user, and technical support among factors affecting systems availability users.

Information Systems Security in Africa

In 2020, the International Telecommunication Union (ITU) released a Global Cyber Security Index (GCI) to establish the cybersecurity posture of a country, organisation, or business. The most commonly identified pallor of Information Security for African countries was found in the legal, technical, organisational, capacity development and cooperation aspect of respective countries. In addition, developed countries (and large organisations) have a sufficient budget for Information Security (Pekin, 2020). However, the same cannot be concluded in African countries. In this case, financial institutions are the most affected as incidences of hacking and fraud increase annually across the world and Africa in particular (Kshetr, 2019).

At the national level, different African countries coordinate efforts to address the challenge of Information Security. Such efforts include providing the legal, and regulatory framework for Information

Security, investigating cybercrimes, dealing with different forms of cyber-attacks, and data protection (International Telecommunication Union, 2021). While the African continent is diverse, some similarities are also shared (Talla & Robert, 2019). The current study capitalised on possible similarities; this is why it synthesised common factors affecting the security of Information Systems within the African continent. Overall, the current study has a unique contribution because it focuses on factors affecting Information Security in Africa. In addition, its contribution is unique because it uses descriptive statistics to prioritise factors affecting the security of Information Systems.

Methodology

This study adopted mixed methods, which include the use of both quantitative and qualitative data and analysis. Within qualitative approach, the study applied a systematic literature review method, with a meta-analysis perspective. The meta-analysis combines results of multiple scientific studies to get the desired result (Deckers & Lago, 2022). This literature review process focuses on objectives rather than evaluating interventions (Deckers & Lago, 2022); therefore, it addresses the purpose of this study. A single subject is observed across selected publications to deduce their position. In the context of the quantitative perspective, the study objectively evaluated, synthesised, and summarised results in Tables 3, 4, and 5, using descriptive statistics. Since this study was based on the review of the literature, it was necessary to select Journal and Conference publications on Information Security conducted in Africa. Other criteria for paper selection include a clear research approach, the relevance of the sampling procedure, the relevance of analysis and the validity of data (refer to Table 4).

Sampling Method

The sample of the study included research papers published between 2010 and 2020. Within this period, many world-crushing security incidents affected large and small businesses (Kshetr, 2019). Other criteria for selected research papers include peer review, not being on the predatory list of publishers, and having its origin in Africa. In addition, sampled papers must identify factors affecting the security of Information Systems within Africa. To obtain relevant papers, the study used the following keywords on the Google search engine: Information Security in Africa and Cybersecurity in Africa. In total, the sample had 70 research articles, which were used to understand the quality of publications in the area of Information Security. Articles that qualified were used in understanding factors affecting the security of Information Systems. Table 1 presents the source of publications.

Table 1: Journals and Conferences Used in the Analysis

Source of Publication	*Number of papers*
Journal of Theoretical and Applied Information Technology	2
Computers & Security	1
Computers in Human Behaviour	2
IEEE	2
Journal of Information and Organizational Sciences,	1
Journal of Computers	2
Scientific and Technical Information Processing	1

Behaviour and Information Technology	1
MIS Quarterly	2
Journal of Information Security	2
Journal of Computer Information Systems	3
International Federation for Information Processing	2
International Journal of Computer Science and Business Informatics	1
Journal of Information Warfare	2
Advances in Intelligent Systems and Computing	2
Journal of Computer Security	2
Fifth Annual Symposium on Information Assurance	1
Computational Inteligence and NeuroCience	1
South African Journal of Information Management	5
5th International Conference on Computing and Informatics	1
Communications of the ACM	1
Malaysian Journal of Computer Science,	1
Journal of Organizational Computing and Electronic Commerce	1
International Journal of Innovations in Engineering and Technology	2
THREAT Conference Proceedings	4
Science and Engineering Ethics,	1
International Conference on Research and Innovation in Information Systems (ICRIIS)	3
Behaviour & Information Technology	1
Social and Behavioural Sciences	1
Proceedings of the Sixth International AAAI Conference on Weblogs and Social Media	1
The African Journal of Information Systems	5
Scuverse Science Direct	2
ICT for Africa	3
Southern African Business Review	1
IST Africa Conference Proceedings	5
4th International Workshop on Socio-Technical Perspective in IS development (STPIS'18)	1
Proceedings of the International Conference on Industrial Engineering and Operations Management Pilsen	1
Total	70

Source: Researchers (2021)

Data Collection

Table 2 summarises the content of the information extracted through the systematic literature review process. To determine the quality aspects of publications on Information Security, this study used criteria identified in sampling methods. Based on these criteria, factors affecting the security of Information Systems in the African continent were identified and tallied. Table 2 used F_1 to F_n to represent the list of recorded factors.

Table 2: Worksheet for Capturing Data

Authors	Year	Paper quality				Factors impacting Information Security			
		Approach	Sampling	Analysis	Validity	F_1	F_2	F_3	F_4
Ada, S., Sharman, R., & Gupta, M.	2010					√	√	√	√

F_1 = Human factors
F_2 = Environment factors
F_3 = Inadequate policy
F_4 = Demographic factors
Source: Researchers (2021)

Data Analysis

The main method of data analysis in this study was descriptive statistics that used frequencies and percentages. This followed after the study captured respective information in the statistical package spreadsheet. To ensure the quality of the current study, the study used the quality criteria checklist from Hassan, Ismail and Maarop (2015) to come up with categories of factors shown in Table 2. These categories are supported by credible publications such as that of Arbanas and Hrustek (2019) and Bolek et al (2016). Furthermore, the criteria for sorting papers to be included in the current sample, as explained above, ensured the validity of the extracted data. Additionally, a collective verification of papers meeting the checklist was necessary to ensure the quality of this study. This is in alignment with the study by Ridzuan and Zainon (2019), who emphasised data cleaning before beginning the analysis process.

Results

This section presents the results of the study. The work is organised based on two aspects: the first aspect is about the quality of Information Security papers with themes from Africa, and the second aspect is about factors affecting the security of Information Systems. The presentation of data on the quality of publications is based on 70 papers from Africa. Among them, only 37 qualified for the analysis of factors affecting the security of Information Systems in Africa. Table 3 provides the summary of all papers that were used to understand the quality of publications on Information Security.

Table 3: Number of Research Papers Published between 2010 and 2020

	Frequency	Percentage
2010	7	9.3
2011	7	9.3
2012	5	7.0
2013	3	4.7
2014	10	14.0
2015	10	14.0

2016	11	16.3
2017	5	7.0
2018	5	7.0
2019	8	11.6
Total	70	100.0

Source: Research Data (2021)

According to Table 3, most of the research articles were published between 2014 and 2016, with a total of 42.2%. This is the period where mega attacks compromised the security of Information Systems across the world. For example, Adobe reported that three million encrypted customer credit cards were attacked, an attack on eBay exposed its entire account list of 145 million users in May 2014, and 6.5 million LinkedIn passcodes were stolen in 2016 (National Cyber Security Center, 2021). Furthermore, 136 million MySpace user accounts were put for sale on the Dark Web in 2016, and Yahoo reported a data breach involving 500 million user accounts in September 2016 at the cost of $350 million (Swinhoe, 2021). Unfortunately, the data concerning African businesses affected in this time window is unavailable; however, statistics show the increase.

The Quality of Research Articles on The Security of Information Systems

This subsection explains the quality of papers included in this research exercise. The current study determined the research approach used and its relevance when related to the relevance of the sampling procedure, the relevance of the analysis procedures, and the validity of data. Table 4 summarises the results.

Table 4: Descriptive Information on the Quality of Research Articles Used in the Study

Quality aspect	Description	Number of research articles	Total percent
Research approach	Qualitative approach	23	32.9
	Quantitative approach	33	47.1
	Mixed approach	14	20.0
Relevance of sampling procedures	Relevant	37	52.9
	Not relevant	33	47.1
Relevance of analysis	Relevant	65	92.9
	Not relevant	5	7.1
Validity of data	Valid	54	77.1
	Invalid	16	22.9

Source: Researchers (2021)

Research Approach

According to Table 4, most of the research papers used the quantitative approach; this is 47.1% of the whole sample. This is likely because the approach is objective and saves time during analysis (Daniel, 2016). Furthermore, the approach makes generalisation possible through the use of scientific methods of data collection (Almeida, Faria, & Queirós, 2017). Moreover, 32.9% of papers were qualitative. Although fewer papers used the qualitative approach, the study is convinced that it played a significant role in generating new knowledge, including researchers' experience in the whole process (Rahman, 2017). Lastly, 20% of the studies used mixed research methods. This study adopted this method as well and assumed that the application of different approaches enriched the research areas with relevant knowledge during this time.

Sampling and Analysis Methods

According to Table 4, 52.9% of all articles used relevant sampling and analysis methods. Their sampling and analysis methods matched the requirement of their research approach. Moreover, 46.6% of articles used irrelevant sampling and analysis methods. These articles used sampling and analysis methods that did not support their chosen research approach. The study by Apuke (2017) suggested probability sampling for quantitative studies. Accordingly, statistical models form a very important base for decision-king in quantitative studies (Rahman, 2017). On the other hand, the study by Mohajan (2018) suggested the following analysis methods to fit in qualitative studies: content analysis, narrative analysis, discourse analysis, framework analysis and grounded theory.

Validity of Data

According to Table 4, 77.1% of all articles affirmed their validity, while the remaining (22.9%) did not. According to these results, most studies in the African continent and the field of Information Security adhere to validity principles. According to Heale and Twycross (2015), quantitative studies use construct validity to determine the validity of data, while qualitative studies use methods such as content validity. Furthermore, Taherdoost (2016) suggested that it is important to select a reliable tool for data collection for valid and relevant data for the study. This would equally enhance the reliability of the study. Reliability and validity are fundamental concepts that help researchers understand how well their measures work and whether data can be trusted (Cypress, 2017).

Factors Affecting the Security of Information Systems

This part focuses its analysis on 37 papers within the Information Security area, published between 2010 and 2020, of African origin. These are the only papers which met the quality criteria. The motivation for the study is the fact that, like the rest of the world, the continent is increasingly reporting security incidents that affect all types of businesses. Therefore, it was the goal of this study to understand why Information System security is still a problem for most organisations, as well as individual users within Africa. The study by Arbanas and Hrustek (2019) recommends the classification of factors affecting Information Systems security into human factors, Information Security policy, work environment and demographic factors. This study categorised factors affecting Information Security based on research papers within Africa, as presented in Table 5 below.

Table 5: Factors Affecting the Security of Information System

Category	Specific factors reported in different papers	Specific factors' Information		Category Information	
		Freq.	Perc.	Freq.	Perc.
Human factor	Lack of skills	8	26.7%	30	20%
	Carelessness	10	33.3%		
	Trust	12	40.0%		
	Subtotal	30	100.10%		
Inadequate Information Security policy	Policy creation	10	33%	30	20%
	Policy implementation	8	27%		
	Lack of IS security training	12	40%		
	Subtotal	30	100.0%		
Work environment	Management support	14	26.9%	52	34.7%
	Organisation Security culture	14	26.9%		
	Workload	12	23.1%		
	Internet and Network Use	8	15.4%		
	Access Control	4	7.7%		
	Subtotal	52	100%		
Demographic factors	Gender	12	42.9%	38	25.3%
	Age	4	14.3%		
	Education level	4	14.3%		
	Work experience	8	28.6%		
	Subtotal	38	100.0%		
Total of Category				150	100%

Source: Researcher (2021)

Human Factors

The study by Alhogail, Mirza and Bakry (2015) considers human factors regarding how people behave physically and psychologically in relation to the security of Information Systems. In addition, the study by Glaspie and Karwowski (2018) emphasised that the success of an organisation's Information Security depends on the appropriateness of user behaviours upon the use of the system. According to the current study, the results of the analysis presented in Table 5 suggested that human factors contribute 20% of all reported factors that impact the security of Information Systems in Africa. Human factors within this category include trust, carelessness, and lack of skills. The next part provides details about the data presented in Table 5.

i.) *Trust*: In this study, trust is the most impactful human factor, as it reports 40% of responses within its category. Moreover, with 12 counts, it is among three factors ranked in third place, which impacts the security of Information Systems based on African publications. One happens to trust another person as the result of recommendations from co-workers or personal experience (Rajaonah, 2017). While trust sounds good, it becomes a point of attack if precautions are not taken (Sapronov, 2020). Some of the risky behaviours associated with trust include sharing data or log-in credentials without security considerations among employees (Astakhova, 2016; Robinson, 2019). These habits lead to more Information Security risks (Brock & Khan, 2017; Boehmer et al, 2015).

ii.) *Carelessness*: Another human factor reported to affect the security of Information Systems in the African context is carelessness. Carelessness reports 10 counts of responses and a total of 33.3% within the human factor category. Carelessness can be considered as an action or behaviour of an individual that knowingly or unknowingly risks the security of the Information System. For example, gossiping about office issues on public networks or emails, as it is estimated that an average cooperate email user sends up to 112 emails every day, and one out of every seven emails (approximately) can be related to office gossips (Mitra & Gilbert, 2012). The carelessness of gossiping about office-related matters on social media can result in unknowingly exposing confidential information to unauthorised/unwanted persons and increase security risk to an organisation. Moreover, other behaviours, such as trusting a visiting guest to use an organisation's computer and connecting personal computer devices to the organisation network without necessary precautions, create security alarms. Additionally, leaving office computers without logging out, introducing new hardware/software to the users without appropriate training, and operating ICT infrastructures without an ICT/IS security policy can create security risks. Furthermore, using outdated software and hardware and so many others are considered careless habits that can jeopardise an organisation's Information Security.

iii.) *Lack of skills:* Table 5 identified the lack of skills as another human factor affecting Information Security in Africa. This factor has 8 counts from the literature, which is 26.7% of responses within the human factors category. Based on the study by Kagwiria (2020), many people lack confidence in their technicians' Information Security skills and knowledge to deal with modern security challenges. This is a challenge as most Information Security certifications are expensive for individuals. Furthermore, most organisations are not willing to sponsor their employees for professional certifications (Fields, Fields, & Patrick, 2016). On the other hand, normal users also lack skills, as indicated in the study by CISCO (2016).

Eventually, this combination affects efforts to ensure the security of Information Systems within Africa (Muller, 2015; Africa Cyber Security Report, 2018).

Inadequate Information Security Policy

An Information Security policy defines the roles and responsibilities of employees in protecting the Information System in an organisation (Bulgurcu, Cavusoglu, & Benbasat, 2010). If followed, policies ensure proper management of technological resources (Watters & Ziegler, 2016). In the current study, this category of factors (affecting Information Security) was reported by 20% of all responses; this percentage is the same as that of human factors. Factors reported to belong to this category (refer to Table 5) are explained further in the next part.

i.) *Lack of Information Security Policy Training*: This is the most reported factor within the policy category. The data in Table 5 report 12 counts from the literature, which is 40% of all responses within the policy category. Training would provide users with appropriate knowledge for ensured security (Ghazvini & Shukur, 2016). Training equips users with reliable tools and knowledge to enforce Information Security within the organisation (Alqahtani, 2017).

ii.) *Poor Creation of Information Security Policies*: This is the second-highest reported factor within the security policy category. It received 10 counts, which is a total of 33.3% of counts within its category of responses. Studies by Lubua and Pretorius (2019) offer frameworks to follow that also suggest minimum requirements for a security policy. They recommend the security policy have the following components: data security, Internet and network services governance, use of the company's own devices, physical security, incident handling and recovery, monitoring and compliance and policy administration. Together with such requirements, Alqahtani (2017) emphasised the importance of involving all security stakeholders in the process of creating the policy. This will enable them to share their opinions in the process of identifying risk areas within the organisation. Engaging key stakeholders while following recommended standards will ensure the formulation of a credible policy (Hina & Dominic, 2018).

iii.) *Poor Implementation of Information Systems Policies*: Poor implementation of Information Security policies is equally identified among factors affecting the security of Information Systems, as shown in Table 5. This factor has 8 counts, with 27% of responses within the policy category. The study by Lopes and Oliveira (2015) suggested that difficulties in policy implementation occur because most policies are developed for compliance purposes; they do not reflect actual security demands. With proper implementation of Information Security policies, the organisation could identify implementation problems, limitations and technical developments that need policy considerations (Alotaib, Alotaib, & Clarke, 2016). The absence of proper policy implementation turns Information Systems policies into inoperative documents; this increases vulnerabilities (Lopes & Oliveira, 2015).

Work Environment

In this paper, the work environment is referred to as social features and physical conditions in which users of Information Systems perform their jobs; this definition is adopted from Greene (2010) and Humaidi and Balakrishnan (2015). In the current study, the work environment is the category of factors mostly reported to affect the security of Information Systems in Africa. It reported 34.7% of all factors cited from studies conducted in Africa. The next part reports individual factors, as reported in Table 5.

i.) *Management Support*: This is one of the two highly reported aspects which impact the security of Information Systems. Within the work environment category, management support has 14 counts from the literature, which is 26.9% of all responses in this category. Senior managers should set an example (in the organisation) by ensuring proper training, awareness programmes and while positively shaping their security behaviour (AlHogail, 2015; Kearney; Kruger, 2016). Other methods for the management to show support to subordinates include idealising security influence in an organisation, individualised consideration and inspirational motivation (Choi, 2016). Management failure to provide support to security programmes increases the vulnerability of the organisation, as observed by Padayachee (2012) and Hassan, Ismail and Maarop (2015).

ii.) *Organisation Security Culture*: This is another highly reported factor for Information Systems security. Like management support, it has 14 counts from the literature, which carries the weight of 26.9% within the work environment category. The culture of the organisation involves the establishment of policies, standards, and guidelines that guide the behaviour of individuals in an organisation (Alhogail, Areej; Mirza, 2014). The failure of the organisation to create the right security culture contributes to the increase of security risks related to Information Systems (AlHogail, 2015; Brock & Khan, 2017). The management of the organisation must create the right security culture and incorporate it into the long-term programme. Unfortunately, studies show this is not the case for some organisations in Africa (Patrick, Niekerk, & Fields, 2018).

iii.) *Workload*: The workload is another factor reported within the category of the work environment. In this paper, the workload is the amount of work that needs to be completed in a given time and resources (Vernon-Bido, Grigoryan, Kavak, & Padilla, 2018). The study found it to constitute 23.1% within its category and 12 counts in total. Studies report that many violations of Information Systems security are the result of the desire of employees to maximise output within limited resources (Arian et al, 2017). Eventually, the pressure applied by the organisation to employees to achieve higher financial goals increases the chance of security violations by employees (Martin, Rice, & Martin, 2016). This is because the persistent pressure to strain resources makes employees ignore security risks in place of performance (Allam, Flowerday, & Flowerday, 2014).

iv.) *Internet and Network Use*: This refers to an organisation's dependence on the Internet and network to carry out its business. It is another factor within the work environment category reported affecting security within Africa. In Table 5, Internet and network use constitute 15.4% within the work environment category; in total, there are 8 counts from the literature about this factor. In today's business environment, the connection to the Internet is inevitable to remain competitive (Khan, Musa & Alshare, 2015; Saunders & Brynjolfsson, 2016). If the organisation uses the Internet to support its business without proper consideration of security risks, the use of the Internet becomes a liability to the security of Information Systems (Tawalbeh et al, 2020).

v.) *Access Control*: Last but not least, in the category of work environment, there is the concept of access control. In this case, the factor is reported to contribute 7.7% of counts within the category of the work environment; it reported 4 counts from the literature. In most cases, access controls weaken as users demand more privileges when working with the system (Sindiren & Ciylan, 2018). The organisation must guide system accessibility based on the roles and responsibilities of an individual rather than simply making someone happy at the cost of overall security (Pesic & Veinović, 2016). Access privileges include read-only, read-and-write and others (Etezady, 2011). Failure to define system access rules exposes such a system to threats (Connolly, Lang, & Tygar, 2014). Access rules are defined through policies and guidelines of the organisation or by overriding industry standards (Mudarri, Al-Rabeei, & Abdo, 2015).

Demographic Factors

This part presents findings of various demographic factors reported to affect the security of Information Systems with the literature based in Africa. Barlow, Warkentin, Ormond and Dennis (2013) suggested that factors such as gender, age, level of education, experience, and managerial role can be used in predicting intention to comply with Information System security. In the African context, the factors presented in Table 5 are the ones sported in the literature. These factors are discussed next.

i.) *Gender*: In this study, gender is reported to affect the security of Information Systems. According to the analysis in Table 5, gender is the most reported demographic factor, with 42.9% of responses. Gender has a total of 12 counts from the literature. With regard to gender, McGill and Thompson (2018) observed that females are more likely to perceive a high level of security threats than males. In another study, Alotaibi and Alshehri (2020) observed that males are likely to show better Information Security behaviours than their female counterparts. Meanwhile, according to Fields, Fields, and Patrick (2016), Information Systems is perceived as a male-dominated field; therefore, there is a need to motivate females to be more involved in undertaking Information Systems security studies and build interest in security careers.

ii.) *Work Experience:* Work experience is the second most reported within the category of demographic variables. The variable has 28.6% of responses within the category of demographic variables and a total of 8 counts from the literature. The assumption is that the experience of an individual with work, both technical and non-technical, relates to the suitability of demonstrated Information Security behaviour. In the study by Erceg (2019), experienced employees are more secure due to their previous encounters in dealing with different security incidents. Furthermore, work experience provides the avenue for training, which provides relevant knowledge for protection against attacks (Connolly, Lang, & Tygar, 2014).

iii.) *The Age of Internet Users*: The age of Internet users is equally reported to affect Internet security within the literature based in Africa. In this study, the age of Internet users forms 14.3% of all identified factors within the demographic category; it has 8 counts in total. In their study, Fatokun et al (2021), showed that younger people are more likely to have cyber security awareness compared to their counterparts. Together with their security awareness, they are equally careless (Levesque, Fernandez, & Batchelder, 2017). Furthermore, young people are easy to teach during new transformations; this is necessary when the organisation transforms its security measures (Fatokun et al, 2021). Based on these findings, it is necessary to increase efforts so as to address the carelessness status of young people while improving the security awareness of adults in Africa.

iv.) *Level of Education*: Insufficient education is reported to affect Information Security by 14.3% in this study, as represented in Table 5 that the level of education has 4 counts in total. Research conducted by Bostan (2015) showed that sharing of information through the Internet within businesses brings various Information Security challenges. These challenges are related to maintaining information confidentiality and integrity depending on the end-user awareness/education level and behaviour. The ability to successfully prevent a nation's critical infrastructure against cyber-attacks depends on a skilled cyber-literate workforce and an education system that can be built such a workforce (Catota, Morgan1, & Sicker, 2019). On the other hand, it is possible to outsource foreign experts. This is not a sustainable solution for African countries and might raise other security matters. Based on these facts, to continue the use of network and Internet infrastructures for businesses and organisations, a nation needs to build its own Information Security workforce by strengthening its education system and focusing on Information System Security and Cyber Security.

Conclusion and Recommendation

This paper synthesised the literature so as to understand key factors affecting the security of Information Systems within Africa. The study reported findings based on the following categories: The first category includes human factors such as carelessness, the level of skills and trust. The second category was the inadequacy of Information Security policies, which includes issues such as policy creation, implementation and the lack of security training. In addition, the study used the category known as work environment; the category includes factors such as management support, organisation security culture, workload and Internet, network usage and access control. Lastly, the study used the category known as a demographic factor, which includes factors based on gender, age, education level, and work experience.

Collectively, the work environment is the category with the highest impact of all; this is followed by demographic factors, inadequate Information Security policies, and human factors. In addition, the following (in their order) are the top factors (from different categories) that had the most impact on the security of Information Systems: gender (women are mostly affected), and the lack of Information Security training. Also, the unchecked level of trust, carelessness and poor security policies. Based on these findings, the study recommends the following: -

i. Organisations should conduct regular training for their employees to enhance their competency in cybersecurity.
ii. Organisations should put deliberate effort into enhancing the knowledge of women since they are mostly affected in Africa. Organisations should develop well-updated policies which comprehensively address modern security concerns.
iii. Organisations should encourage behaviours that decrease exposure to security risks.

Since the literature showed a direct lack of a common point of reference on the factors affecting the security of information systems, particularly in the African context, the study established that point of reference for the body of knowledge. However, it is the limitation of this study that it focuses only on factors affecting the security of information systems in an African context. Further studies can be done to investigate factors affecting the security of information systems in other countries around the world and identify other factors that affect the security of information systems in different organisational settings in different countries.

References

Ada, S., Sharman, R., & Gupta, M. (2009). Theories Used in Information Security Research; Survey and Agenda. *IGI Global*, 270-292.

Africa Cyber Security Report. (2018). *Cyber Security Skill Gap.* United States Internationa University-Africa.

Alhogail, A., Mirza, A., & Bakry, S. H. (2015). A Comprehensive human factor framework for information security in organizations. *Journal of Theoretical and Applied Information Technology, 78*(2), 201-211.

Alhogail, Areej Mirza. (2014). A framework of information security culture change. *Journal of Theoretical and Applied Information Technology*, 64(2), 540-549.

Allam, S., Flowerday, S., & Flowerday, E. (2014). Smartphone Information security awareness: A victim of operational pressures. *Computers & Security*, 42, 56-65.

Almeida, F., Faria, D., & Queirós, A. (2017). Strengths and limitations of qualitative and quantitative research methods. *European Journal of Education Studies, 3*(9), 369-387.

Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). Security policy compliance: User acceptance perspective. *IEEE*, 45(12), 1-10.

Alotaib, M., Alotaib, M., & Clarke, N. L. (2016). Information security policies: A review of challenges and influencing factors. *11th international conference for internet technology and secured transactions*, (pp. 1-7).

Alqahtani, F. H. (2017). Developing an information security policy: A case study approach. *4th Information Systems International Conference* (pp. 691-697). Bali, ISICO.

Ana-Maria, S., & Bîzoi, M. (2010). Audit for Information systems security. *Informatica Economica,* 14(1), 40-48.

Apuke, O. D. (2017). Quantitative research methods : A synopsis approach. *Arabian Journal of Business and Management Review (Kuwait Chapter),* 6(10), 40-46.

Arbanas, K., & Hrustek, N. Ž. (2019). Key success factors of information systems security. *Journal of Information and Organizational Sciences,* 43(3), 131-144.

Arian, T., Kusedghi, A., Raahemi, B., & Akbari, A. (2017). A Collaborative load balancer for network intrusion detection in cloud environments. *Journal of Computers, 12*(1), 28-47.

Astakhova, L. V. (2016). The Ontological Status of Trust in Information Security. *Scientific and Technical Information Processing,* 43(1), 58-65.

Bagchi, K. K., & Udo, G. (2003). An Analysis of the growth of computer and internet security breaches. *Communications of the Association for Information Systems*, 684-700.

Bai, Z., Jain, N., Kurdyukov, R., Walton, J., Wang, Y., Wasson, T., . . . Chircu, A. M. (2019). Conducting sysematic literature review in information system: An analysis of guidelines. *Issues in Information Systems,* 20(3), 83-93.

Boehmer, J., Larose, R., Rifon, N. J., Cotten, S. R., & Alhabash, S. (2015). Determinants of online safety behaviour: Towards an intervention strategy for college students. *Behaviour and Information Technology,* 34(10), 1-14.

Boell, S. K., & Wang, B. (2019). An IT Artifact supporting exploratory literature searches for information systems research. *Australasian Conference on Information Systems* (pp. 1-12). Sydney: Australasian Conference on Information Systems.

Bolek, V., Látečková, A., Romanová, A., & Korcek, F. (2016). Factors affecting information security focused on sme and agricultural enterprises. *Agris On-line Papers in Economics and Informatics,* 8(4), 37-50.

Bostan, A. (2015). Impact of education on security practices in ICT. *Tehnicki Vjesnik, 22*(1), 161-168.

Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective. Part I: The Causes. *Management Information Systems Research Center,* 1(3), 17-32.

Brock, V., & Khan, H. U. (2017). Big data analytics: Does organizational factor matters impact technology acceptance? *Journal Of Big Data, 4*(1), 1-28.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly,* 34(3), 523-548.

Catota, F. E., Morgan1, G., & Sicker, D. C. (2019). Cybersecurity Education in a developing nation: The Ecuadorian environment. *Journal of Cyber Security*, 1-19.

Charitoudi, K., & Blyth, A. (2013). A Socio-Technical approach to cyber risk management and impact assessment. *Journal of Information Security*, 4(1), 33-41.

Choi, M. (2016). Leadership of Information security manager on the effectiveness of information systems security for secure sustainable computing. *Sustainability* , 8(7), 6-38.

CISCO. (2016). *Mitigating the Cybersecurity Skills Shortage* . sunfrancisco: CISCO.

Cohen, J., & Nagin, D. S. (1978). General deterrence: A review of the empirical evidence. *National Academy Press*, 95-139.

Connolly, L., Lang, M., & Tygar, D. (2014). Managing Employee security behaviour in organisations: The role of cultural factors and individual values. *International Federation for Information Processing*, 417-428.

Cvitić, I., Perakovic, D., & Kuljanić, T. M. (2017). Availability Factors in delivery of information and communication resources to traffic system users. *Communications in Computer and Information Science* , 1-3.

Cypress, B. S. (2017). Rigor or Reliability and validity in qualitative research: Perspectives, Strategies, reconceptualization, and recommendations. *Dimensions of Critical Care Nursing,* 36(4), 253-263.

Daniel, E. (2016). The usefulness of qualitative and quantitative approaches and methods in researching problem-solving ability in science education curriculum. *Journal of Education and Practice*, 7(15), 9-100.

Deckers, R., & Lago, P. (2022). Systematic literature review of domain-oriented specification techniques. *Journal of Systems and Software*, *192*, 1-11.

Dieser, A., Covella, G. J., & Olsina, L. (2014). Specifying Security Characteristics, Attributes, and Metrics for Evaluating Web Applications. *2do Congreso Nacional de Ingeniería Informática / Sistemas de Información (CoNaIISI)*, (pp. 1-12). San Luis, Argentina.

Erceg, A. (2019). Information security: Threat from employees. *Tehnički Glasnik, 13*(2), 123-128.

Etezady, N. (2011). The impact of ERP investments on organizational performance. *International Journal of the Academic Business World,* 5(2), 27-33.

Fatokun, F. B., Hamid1, S., Norman, A., & Fatokun, J. O. (2021). The impact of age, gender, and educational level on the cybersecurity behaviors of tertiary institution students: An empirical investigation on Malaysian Universities. *International Conference Computer Science and Engineering* (pp. 1-13). Kuala Lumpur, Malaysia: IOP Publishing Ltd.

Fields, Z., Fields, Z., & Patrick, H. (2016). Security-information flow in the south african public sector. *Journal of Information Warfare*, 15(4), 68-85.

Flowerday, S., & Tuyikeze, T. (2016). Information security policy development and implementation: the what, how and who. *Computers & Security,* 61, 169-183.

Ghazvini, A., & Shukur, Z. (2016). Awareness Training transfer and information security content development for healthcare industry. *International Journal of Advanced Computer Science and Applications*, 5(7), 361-370.

Glaspie, H. W., & Karwowski, W. (2018). Human Factors in information securityculture: A literature review. *Advances in Intelligent Systems and Computing,* 8(1), 269-281.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The Impact of information security breaches: has there been a downward shift in costs? *Journal of Computer Security*, 19(1), 33-56.

Grant, M. J., & Booth, A. (2009). A typology of reviews: An analysis of 14 review types and associated methodologies. *Health Information and Libraries Journal*, 26, 91-108.

Greene, G. (2010). Assessing the impact of security culture and the employee-organization relationship on is security compliance I. *Fifth Annual Symposium on Information Assurance.* New York.

Han, D., Dai, Y., Tianlin Han, & Dai, X. (2015). Explore Awareness of information security: Insights from cognitive neuromechanism. *Computational Inteligence and NeuroCience* , 1-11.

Hassan, N. H., Ismail, Z., & Maarop, N. (2015). Information security culture, a systematic literature review. *The 5th International Conference on Computing and Informatics*, (pp. 456-463). Instanbul.

Heale, R., & Twycross, A. (2015). Validity and Reliability in Quantitative Research. *Evidence-Based Nursing*, 18(3), 66-67.

Helpnetsecurity. (2020). *445 Million Attacks Detected Since the Beginning of 2020, COVID-19 Wreaks Havoc.* Helpnetsecurity.

Hina, S., & Dominic, D. D. (2018). Information Security policies’ compliance:A perspective for higher education institutions. *Journal of Computer Information Systems*, 60(3), 1-11.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does Deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, 54(6), 54-90.

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

International Monetary Fund. (2021). *Reginal Economic Outlook: Sub-Saharan Africa.* IMF.

International Telecommunication Union. (2021). *Cyber Security in Tanzania – Country Report.* ITU.

Kagwiria, C. (2020). *Cyber Security Skills Gap in Africa.* Nairobi: AFRALIT.

Kaspersky. (2020, october 17). How Data Breaches Happen: What they are and Why it Matters. https://www.kaspersky.com/resource-center/definitions/data-breach

Kaspersky. (2020). *Top Ransomware Attacks of 2020.* Moscow-Russia: Kaspersky.

Khan, H. U., & AlShare, K. A. (2019). Violators versus non-violators of information security measures in organizations: A study of distinguishing factors. *Journal of Organizational Computing and Electronic Commerce*(1), 4-23.

Khan, Musa & Alshare. (2015). Factors influence consumers’ adoption of mobile payment devices in Qatar. *International Journal of Mobile Communications, 13*(6), 670-689.

Kruger, K. (2016). Can Perceptual differences account for enigmatic information security behaviour in an organisation? *Computers & Security*, 61, 46-58.

Kshetr, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*, 22(2), 77-81.

Kumar, R. (2011). *Research Methodology: A Step by Step Guide for Biginners.* SAGE Publications India Pvt Ltd.

Levesque, F. L., Fernandez, J. M., & Batchelder, D. (2017). Age and gender as independent risk factors for malware victimisation. *Digital make-believe.* Sunderland, UK.

Limaye, R. (2013). The importance of information integrity. *International Journal of Innovations in Engineering and Technology, 2*(3), 274-281.

Lopes, I., & Oliveira, P. (2015). *Implementation of Information Systems Security Policies:A Survey in Small and Medium Sized Enterprises* . Bragança, Portugal : Springer International Publishing.

Lubua, E. W. (2014). Cyber Crimes Incidents in Financial Institutions of Tanzania. *International Journal of Computer Science and Business Informatics, 14*(3), 37-48.

Lubua, E. W., & Pretorius, P. D. (2019). Cyber-security policy framework and procedural compliance in public organisations. *Proceedings of the International Conference on Industrial Engineering and Operations Management* (pp. 1847-1856). Pilsen, Czech Republic: IEOM Society International.

Lubua, E. W., & Pretorius, P. D. (2019). Ranking Cybercrimes Based on Their Impact to Organisations' Welfare. *THREAT Conference Proceedings* (pp. 1-11). Johannesburg: THREAT.

Lueg, C. P. (2001). Information dissemination in virtual communities as challenge to real world companies. *Towards The E-Society: E-Commerce, E-Business, and E-Government, The First IFIP Conference on E-Commerce, E-Business, E-Government* (pp. 1-11). Zürich, Switzerland: E-Society: E-Commerce, E-Business, and E-Government, The First IFIP Conference on E-Commerce, E-Business, E-Government.

Lundgren, B., & Möller, N. (2017). Defining information security. *Science and Engineering Ethics, 25*(3), 1-8.

Mahfuth, A., Yussof, S., Baker, A. A., & Ali, N. (2017). A systematic literature review: Information security culture. *International Conference on Research and Innovation in Information Systems (ICRIIS),*, (pp. 1-6). Langkaw.

Manaseer, S., & Alawneh, A. (2019). Cyber security auditing awareness: case of information and communication technology sector. *International Journal of Computer Science and Information Security, 17*(7), 1-7.

Martin, N., Rice, J., & Martin, R. (2016). Expectations of privacy and trust: Examining the views of IT professionals. *Behaviour & Information Technology, 35*(6), 500-510.

McGill, T., & Thompson, N. (2018). Gender differences in information security perceptions and behaviour. *Australasian Conference on Information Systems*, (pp. 1-10). Sydney.

Metalidou, E., Marinagi, C. C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. A. (2014). The human factor of information security: Unintentional damage perspective. *Procedia - Social and Behavioral Sciences, 147*, 424-428.

Metivier, B. (2017, April 17). *Sage advice : Cybersecurity Blog*. https://www.tylercybersecurity.com/blog/fundamental-objectives-of-information-security-the-cia-triad#:~:text=Confidentiality%2C%20integrity%2C%20and%20availability%20(,of%20an%20information%20security%20program.&text=C.,wondering%20which%20is%20most%20imp

Mir, S. Q., Mohammad, S., & Quadri, K. (2016). Information availability: An insight into the most important attribute of information security. *Journal of Information Security*, 185-194.

Mitra, T., & Gilbert, E. (2012). Have you heard?: How gossip flows through workplace email. *Proceedings of the Sixth International AAAI Conference on Weblogs and Social Media* (pp. 242-249). Dublin, Ireland, Spain: The AAAI Press,.

Mohajan, H. K. (2018). Qualitative research methodology in social sciences and related subjects. *Journal of Economic Development, Environment and People,, 7*(1), 23-48.

Mudarri, T., Al-Rabeei, S. A., & Abdo, S. A.-R. (2015). Security fundamentals: access control models. *International Journal of Interdisciplinary in Theory and Practice, 7*(2), 259-262.

Muller, L. P. (2015). *Cyber Security Capacity Building in Developing Countries; Challenges and Oportunities.* Norwegian Institute of International Affairs .

National Cyber Security Center. (2021). *linkedln Hack.* National Cyber Security Center.

Onwuegbuzie, A. J., Leech, N. L., & Collins, K. M. (2012). Qualitative analysis techniques for the review of the literature. *The Qualitative Report, 17*(56), 1-28.

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers and Security,* 10(2), 1-8.

Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010). *Human Factors and Information Security: Individual, Culture and Security Environment.* Edinburgh South Australia 5111 Australia: Department of Defence = Australia.

Patrick, H., Niekerk, B. v., & Fields, Z. (2018). Information security management: A South African public sector perspective. *Journal of Information Warfare,* 15(1), 1-14.

Pekin. (2020). *10 Data Security Methods for Protecting Your Small Business.* Pekin Insurance .

Pesic, D., & Veinović, M. Đ. (2016). Privileged identities: Threat to network and data security. *International Scientific Conference on ICT and e-Business related research*, (pp. 154-160). Belgrade.

Pooe, A., & Labuschagne, L. (2011). Factors Impacting on the adoption of biometric technology by south african banks: An empirical investigation. *Southern African Business Review, 15*(1), 119-138.

Popescul, D. (2011). The confidentiality – integrity – accessibility triad into the knowledge security. a reassessment from the point of view of the knowledge contribution to innovation. *Proceedings of The 16th International Business Information Management Association Conference* (pp. 1338-1345). Kuala Lumpur,: Proceedings of The 16th International Business Information Management Association Conference.

Predd, J., Pfleeger, S. L., Hunker, J., & Bulford, C. (2010). Insiders behaving badly. *IEEE Security & Privacy, 6*(4).

Rahman, M. S. (2017). The Advantages and disadvantages of using qualitative and quantitative approaches and methods in language "testing and assessment" research: A literature review. *Journal of Education and Learning;, 6*(1), 102-112.

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*(1), 109-133.

Ridzuan, F., & Zainon, W. M. (2019). A Review on data cleansing methods for big data. *The Fifth Information Systems International Conference 2019* (pp. 731-73). Procedia Computer Science.

Robinson, S. C. (2019). Factors Predicting attitude toward disclosing personal data online. *Journal of Organizational Computing and Electronic Commerce,* 28(3), 214-233.

Safa, N. S., & khaka, M. S. (2015). Information Security conscious care behaviour formation in organizations. *Computers & Security, 53*, 65-78.

Sapronov, K. (2020). The Human Factor and Information Security. *Kaspersky*.

Saunders, A., & Brynjolfsson, E. (2016). Valuing Information technology related intangible assets. *MIS Quarterly, 40*(1), 50-110.

Sausalito, C. (2020). *Cybercrime To Cost The World $10.5 Trillion Annually By 2025.* New York: Cybercrimme Magazine.

Shahri, A. B., & Mohanna, S. (2016). The Impact of the security competency on "self-efficacy in information security" for effective health information security in Iran. *the Advances in Intelligent Systems and Computing, 445,* 51-65.

Sindiren, E., & Ciylan, B. (2018). Privileged Account management approach for preventing insider attacks. *International Journal of Computer Science and Network Security*, *18*(1), 31-42.

Swinhoe, D. (2021, june 08). *CSO United States*. https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

Taherdoost, H. (2016). Sampling methods in research methodology: How to Choose a sampling technique for research. *SSRN Electronic Journal, 5*(2), 18-27.

Taherdoost, H. (2016). Validity and reliability of the research instrument. *SSRN Electronic Journal, 5*(3), 28-36.

Talla, L. T., & Robert, K. K. (2019). Factors Influencing adoption of information security in information systems projects. *Dynamic Programming for Impulse Feedback and Fast Controls*, 890-899.

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT privacy and security: Challenges and solutions. *Applied Sciense*(10), 1-17.

Thorwat, S. R. (2018). ICT in higher education: Opportunities of urban colleges and challenges of Tribal Colleges. *International Research Journal of Multidisciplinary Studies* , 1-6.

UNODC. (2016). *Global Cyber Security Capacity Centre*. Doha: UNODC.

UNODC. (2020). *Cybersecurity Posture*. Doha: UNODC.

Vernon-Bido, D., Grigoryan, G., Kavak, H., & Padilla, J. (2018). Assessing the Impact of cyberloafing on cyber risk. *Annual Simulation Symposium 2018*, (pp. 1-9). Baltimore, USA.

Watters, P. A., & Ziegler, J. (2016). Controlling information behaviour: The case for access control. *Behaviour & Information Technology, 35*(4), 268-276.

Zoto, E., Kowalski, S., Lopez-Rojas, E. A., & Kianpour, M. (2018). Using a Socio-Technical Systems Approach to Design and Support Systems Thinking in Cyber Security Education. *4th International Workshop on Socio-Technical Perspective in IS development (STPIS'18)*, (pp. 123-128). Tallinn, Estonia.