The International Journal of Engineering and Science (IJES)
|| Volume || 10 || Issue || 11 || Series I || Pages || PP 21-29 || 2021 ||
ISSN (e): 2319-1813 ISSN (p): 20-24-1805

Factors Affecting the Security of Information Systems: A Literature Review

[1]Adam A. Semlambo, *The Open University of Tanzania*
[2]Dr. Catherine G. Mkude, *Department of Information and Communication Technology, The Open University of Tanzania,*
[3]Dr. Edison WazoelLubua, *Department of Informatics, Institute of Accountancy Arusha*

----------***ABSTRACT***----------
Information System Securityis critical to all modern computer users (individuals and organizations). To insure that information remain secure, many organizations implemented various security structure to protect IS security from malicious incidents by establishing security procedures, processes, policies and information system security organization structures. However, despite of all the measures, information security is still a catastrophe. Poor understanding of information security key factor seem to be the main problem. The difference in ICT infrastructure and implementations as well as usage results into different security problems in different organizations. Its eminent that common problem which challenge information security system to all organizations are identified and analysed. Through literature synthesis, this paper discuss common factors affecting the security of information system to modern computer users, which include organizations and individuals. Therefore, helping in saving time and money by focusing the limited resources on elements that really distress IS security.

Keywords*; Information Security, Information System Security, ICT*

Date of Submission: 10-11-2021 Date of Acceptance: 25-11-2021

I. INTRODUCTION

Information Security is the state of being protected against 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 breaches, data loss, cyber security attacks and 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 10.5 trillion US$ by 2025 (Sausalito, 2020). This loss is equivalent to a quota of the budget of a country like Tanzania (with above 55 million people) as reported by its government in the 2020/2021 financial budget(URT, 2020). It is unarguable that resources, which could be used to enrich the standard of living of people is wasted through criminal schemes because of inadequate electronic protection.

Literature and international reports present vast data on Information Security across the world.Helpnetsecurity has recently reported about 445million attacks detected in 2020 (Helpnetsecurity, 2020).The study by ITU (2020)reports that 50% of internet users acknowledge being victims of security breach, LIFARS (incidence response and digital forensics firm)estimates that 29% of organisations that experience Information Security breaches end up losing revenue because of impact of criminal activities(LIFARS, 2020). Collectively, it is evident that cyber-attacks are ever increasing; therefore, the knowledge of factors affecting the Security of Information Systemremains to be significant among the stakeholders.

Literature provides various studies by different researchers about factors that affectIS security(Alhogail, Mirza, & Bakry, 2015; Alhogail, Areej; Mirza, A., 2014; Allam, Flowerday, & Flowerday, 2014; Arbanas & Hrustek, 2019).Al-Omari, El-Gayar and Deokar (2012) analyses factors that affect IS security by focusing on users complience to ICT policies. AlHogail (2015,) focuses on security culture as a factor toward the protection of organizatio IS security, while Alhogail, Mirza and Bakry (2015) developed a framework to only deal with human factor in protection of IS security. Arbanas and Hrustek (2019) almost tolks about all the factors that affect IS security of organizations with disregard to human factor which is very important when talking about IS security to modern ICT users. Hence,the key objective of this paper is to dteremine common factors that affect IS securityto all modern computer users in African context (individuals and organizations (public/Private)), through literature synthesis.

The paper starts with the introduction in section 1, followed by analysing the attributes of organization IS security in section 2, then discuss various IS security theories in section 3. Section 4 talks about methodology of the study, proceeds to results in section 5. Section 6 covers the discussions of findings where common factors that affect IS security are analysed, and conclusion is in section 7.

II. ATTRIBUTES OF ORGANISATIONAL INFORMATION SYSTEM SECURITY

Organization data protection process is a tedious and expensive job, organization faces many challenges in case of data breach. Data breach in organization is estimated to cost 3.92 million US$ with an average data breach of 25,575 records per year as reported in IBM Cost of Data Breach Report (2020) as well as ITU, Global Cybersecurity Index (GCI), (2017).). Also, it may deteriorate trust and lead to investors and customers refraining from doing business with the affected organizations (Gordon, Loeb, & Zhou, 2011). Organizations needs to have the right IS security controls in place to guard against cyberattacks and insider threats while providing document security and insure data availability at all times. It is important to understand IS security attributes so as to evaluate what need to be protected in organization's IS. The IS security basics/attributes includes Confidentiality, Integrity and Availability (CIA) which are the focus of any organization's Information Security Policy(Dieser, Covella, & Olsina, 2014; Mir, Mohammad, & Quadri, 2016).

Source; (Metivier, 2017)

Confidentiality of information refers to the protection of information which covers access controls and measures that protect information from getting misused by unauthorised part or insider threats. Confidentiality can be attained through encryptions, password, two-factor authentication and biometric verification (Mir, Mohammad, & Quadri, 2016). Integrity refers to accuracy and completeness of data, the aim is protecting data from being misused and modified by unauthorised part. Integrity of information can be obtained through encryption, user access control, version control, backup and recovery procedures and error detection software(Dieser, Covella, & Olsina, 2014). Availability is associated with accessibility of data and information to authorised user only. Availability can be attained by offsite backups, disaster recovery, redundancy, failover, proper monitoring, environmental control, virtualization, server clustering and continuity of operational planning (Dieser, Covella, & Olsina, 2014; Mir, Mohammad, & Quadri, 2016). Most of organization, particularly in African fails to identify these IS security attribute, hence fails to protect or have poor protection which resulting into increase of IS security breaches (ITU, 2017; Fields, Fields, & Patrick, 2016)

III. INFORMATION SYSTEM SECURITY THEORIES

Many theories have been used by many researchers in a quest to find solutions for challenges that affect the security of information system (Zoto, Kowalski, Lopez-Rojas, & Kianpour, 2018; Charitoudi & Blyth, 2013; Shahri & Mohanna, 2016; Han, Dai, Tianlin Han, & Dai, 2015; Lubua & Pretorius, 2019). Understanding various IS security theories and their contributions, helps in understanding the IS security literature and identifying factors that affect IS security of organization. The most commonly used IS security theories are socio technical theory, distribute cognitive theory and general deterrence theory.

Social Technical Theory

This theory, consider human factor to be the key point in information security detection and prevention while currently information security is mostly perceived to be a technical issue (Zoto, Kowalski, Lopez-Rojas, & Kianpour, 2018; Charitoudi & Blyth, 2013). Social technical theory is effective in mouldering system security and its environment by examining culture, usability problem, security internal control and security requirement (Zoto, Kowalski, Lopez-Rojas, & Kianpour, 2018; Charitoudi & Blyth, 2013).. Hence, social technical theory

can be used to analyse how people/humans can be contributing factors to IS security based on their perception and approach to organization IS security.

Distributed Cognitive Theory

The theory concentrate on self-efficient process by consigning with how a person can use the skills rather what kind of skills a person has, hence it can be used in information system security as security self-efficiency (Shahri & Mohanna, 2016). The theory propose collaboration among individual to achieve common goal, hence information system security should consign with human cognitive as information is distributed more in a virtual environment (Han, Dai, Tianlin Han, & Dai, 2015).

General Deterrence Theory

This theory was adopted to information system security for the intention of instilling fear of consequence to individuals to discourage an action that will threat the security of information system(Hu, Xu, Dinev, & Ling, 2011). As the theory based in Certainty of sanctions, and severity of sanctions, it proposes set of actions/punishment to be undertaken based on the seriousness of the unlawful action performed by an individual against information security. This theory is important to information security as hacking into IT has become a game or sport and something has to be done as this cost an estimation of up to 2.7 billion US dollars annually (Lubua & Pretorius, 2019; Hu, Xu, Dinev, & Ling, 2011).

From all the theories discussed above. Social technical theory seem to be more appropriate as lack of knowledge about information system security is a contributing factor to all other factors that affect the security of information system. However, despite of all the effort made by different researchers in proposing various theories that can be beneficial in protection of information system security, the theories did not point out what are the real factors to the cause of the actual problems before trying to fix it. A critical analysis and synthesis of literature in IS security is still eminent so that to determine and understand the cause of IS security breach. This will help individuals and organizations to save time and money while directing their limited resources to the actual factors for IS security breaches.

IV. METHODOLOGY

This study will follow a literature review process/secondary study, to complete this study threepublic and available well known databases and search engines namely *Google*, *Wikipedia* and *Google scholar*were involved. The keywords used for querieswereinformation security, information system security, information security culture, organization information security, factor affecting or influencing information security, Cybersecurity, information security review or measurement or analysis or evaluation. The study will follow this criteria as presented below,

Table 1: Summary of Review

Population	Individuals and any organization
Intervention	Information system security
Comparison	None
Outcomes	Factors affecting IS security.
Context	Review (s) of any empirical study of information system security within the domain of any applied case study settings of any organization or individual. No restriction on the type of study applied.

Research questions

This study is guided by the following research questions;

RQ1; Why IS security is still a catastrophe in many organizations regardless of efforts taken to control it?

RQ2; Whatare the factors affecting the IS security of modern computer users?

Study selection and research resources

Based on the identified research questions, a study selection criteria must be conducted to support direct evidence to reduce bias. After the completion of primary research phase, this study follows the research guideline as suggested by Pan and Tomlison (2016). The reference on the selected papers on the primary search phase are thoroughly reviewed, if the paper meets the criteria of selection, will be included in the synthesis. Three well known search engines and databases were used as indicated earlier with the named search terms.

Inclusion and exclusion criteria

The main criteria of this research is to include any study about information security. Either to individual users or any organization. Paper published from 2010 and beyond are taken into consideration for inclusion in this research criterion. The criteria for inclusion are;

- Studies that investigate implementations of information security
- Studies that investigate organizations information security culture.
- Studies that measure effectiveness of organization information security

- Studies that investigate information security key success factors/elements
- Studies that investigate Cybersecurity in organization

Meanwhile, the excluded studies from our research criteria;

- Papers that claim other authors have no supporting evidence
- Papers that are not written in English

Data extraction and study quality assessment (validity and liability check)

To insure the data extraction process meet the criteria, study checklist need to be prepared accordingly(Mahfuth, Yussof, Baker, & Ali, 2017; Hassan, Ismail, & Maarop, 2015). Following that, this study reuse the quality criteria checklist from Hassan, Ismail and Maarop (2015) as presented in table 2 bellow.. This study checklist uses three scales, which are coded and given a score which are Yes = 1, No = 0 and Probably = 0.5. From the item checklist, each paper total score will be calculated by giving a sum from each of the checklist item. Possible score range from 0.5 to a maximum of 5.

Table 2; Item Study Checklist

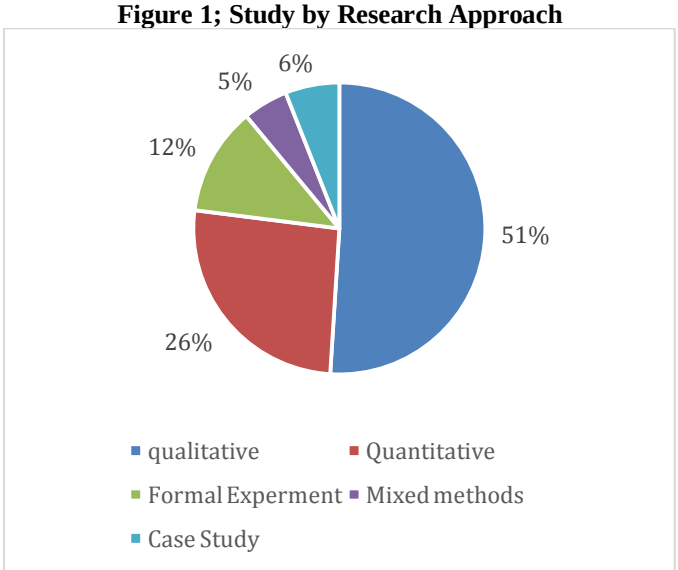
	Item	Answer
01	Was the article referred?	Yes/No
02	Was the aim of the study clearly stated?	Yes/No/Probably
03	Were data collection well carried out?	Yes/No/Probably
04	Were the study participants described?	Yes/No/Probably
05	How generalizable are the findings of the study to the target population with respect to the size and representation of sample.	Yes/No/Probably

V. RESULTS

This section includes the results of findings based on the literature synthesis and research criteria mentioned earlier. The first criterion involves searching for the keywords identified from journal databases and different search engines. Afterwards, two iteration process were used which is primary search that produce 23 final primary studies. In second iteration, the reference contained in the paper are identified in the first iteration are examined. Each of these papers were filtered based on the inclusion and exclusion criteria identified, before included for the synthesis. After reading the titles and abstract and conclusions of the paper and find its relevance to this study, then the full paper will be included for the synthesis. After screening the titles and abstracts, 43 papers were identified.

An analysis of type of studies are presented in figure 1 which based on suggested research type. The percentage of studies screened and sorted for synthesis were 51% of quantitative study papers, 26% qualitative based papers, 12% of formal experiment papers, 5% mixed methods and 6% case studies papers.

Figure 1; Study by Research Approach



Source; Researcher

Quality Factor

The evaluation of synthesis based on quality score is shown in table 3, table 1 show quality score for all primary studies. Most of the studies conducted are in good quality criteria. 15 studies (35%) and 5 (12%). Were deemed good and very good quality respectively. Three studies are in a very poor quality as they did not provide

a detailed result and methodology conducted in their study. These studies were removed in the analysis phase. Thus in the end only 40 papers were included for the purpose of analysis of evidence.

Table3. Results of Quality Checklist

Quality Scale	Very Poor (>=1)	Poor (>=2)	Fair (>=3)	Good (>=4)	Very Good (>-5)	Total
Number of Studies	3	10	10	15	5	43
Percentage	7%	23%	23%	35%	12%	100%

VI. DISCUSSION

In this section, we discuss and represents our findings based on the literature synthesis of 40 of publications in journal articles, conference and research reports as well as books.

What are the factors that affect the security of information system?

From the literature review, 40 information security studies on different public and private sectors as well individuals by different professional on those areas have been identified. The goals was to understand whyIS security is still a problem to most organizations as well as individual users of modern technology. From the synthesis, four factors were identified: human factor, Unreliable information security policy, work environment and demographic factors. Table 3 demonstrate the results from different studies conducted, representing the four factors;

Table 3. Factors Affecting the Security of Information System

Key Factors	**Literature in which the key factor is mentioned**
Human factors	Alavi, Islam, Jahankhani, & Al-Nemrat, 2013, Hassan, Ismail, &Maarop, 2015. Kavuta&Nyamanga, 2018. Mahfuth, Yussof, Baker, & Ali, 2017. Parsons, McCormac, Butavicius, & Ferguson, 2010. Glaspie(&Karwowski, 2018. Sapronov, 2020.
Information security policy	Kasita&Laizer, 2013. Lubua&Maharaj, 2014. Martin, Rice, & Martin, 2016. Uwem& Khan, 2016; Johnston, Warkentin, McBride, & Carter, 2017, Watters & Ziegler, 2016. Bulgurcu, Cavusoglu, &Benbasat, 2010. Park, Kim, & Park, 2017; Vance, Siponen, &Pahnila, 2012. D'Arcy, Herath, &Shoss, 2014; Knapp & Ferrante, 2012. Tamjidyamcholo, Baba, &Tamjid, 2013. Brink, 2011. Hu, Xu, Dinev, & Ling, 2011; Humaidi&Balakrishnan, 2015.
Work environment	Alhogail, Mirza, &Bakry, 2015; Jatau, 2014; Kabanda, Tanner, & Kent, 2018. Greene, 2010; Humaidi&Balakrishnan, 2015. AlHogail, 2015,;W.D.Kearney&H.A.Kruger, 2016. Padayachee, 2012; Predd, Pfleeger, Hunker, & Bulford, 2010; Hassan, Ismail, &Maarop, 2015. Hu, Dinev, Hart, & Cooke, 2012; Khan, Habib Ullah; Lalitha, V.V. Madhavi; Omonaiye, Joseph Funsho, 2017. Allam, Flowerday, &Flowerday, 2014. Martin, Rice, & Martin, 2016.
Demographic factors	Bulgurcu, Cavusoglu, &Benbasat, 2010. Parsons, Kathryn; McCormac, Agata; Butavicius, Marcus; Pattinson, Malcolm; Jerram, Cate, 2014. Ferdani&Hovav, 2014.

VI.1 Human Factor

Human's factor represents employees, management and user and how they behave physically and psychological in relation to organizations IS security(Alhogail, Mirza, & Bakry, 2015). The success of an organization information system depends on the appropriate user behaviour (Glaspie & Karwowski, 2018). Users want security and flexibility and finding the balance between the two is a challenge that every organization has to face (Metalidou, et al., 2014). There is a constant battle between attackers and security system, where user can swing the balance one way or the other by becoming part of IS security attackers or defence system of organization. Unfortunately, the predictability or unpredictability of human behaviour can turn the most secure IS security into nothing (Metalidou, et al., 2014). It is widely perceived that employee of an organization are the weakest link in the protection of IS security (Metalidou, et al., 2014). Providing employees with appropriate training about IS security can turn organization employees into strong defence line against breaches(Sapronov, 2020).

Trust, refers to the willingness of users to share work related data/information with colleagues. Trust is essential in working environment for getting things done; however, it can be misused and lead into risk habits such as sharing of login credentials (username/password) (Astakhova, 2016; Robinson, 2019). This habit eventually leads to more information security risk behaviour and implicates organizations into series of security risk (Brock & Khan, 2017; Boehmer, Larose, Rifon, Cotten, & Alhabash, 2015). Information security survey conducted in the US, UK and Australia that involved 2500 people found that, 40% of users have shared their login credentials within the last 12 months (Khan & AlShare, 2019). It is estimated that, an average cooperate email user sends up to 112 emails every day and one out of every seven email (approximately) can be related to office gossips (Mitra & Gilbert, 2012). Staff engaging in gossips can intentionally or unintentional disclose sensitive or personal information to colleague that they trust, this does not only break information system policy,

but also the low (Martin, Rice, & Martin, 2016). Hence, understanding how trust can be used against organization IS security is critical.

Privacy, in this paper is defined as the intention of an individual to protect/reveal one's or other people's personal information. Security breaches and privacy interruptions costs lots of money to the organizations (IBM Cost of Data Breach Report, 2020). As technology changes day by day, it is very important to maintain various measures of information security to attain organization/individual privacy (Lin, 2016; Chen, Chen, & Wu, 2011). Study done by CISCO revealed that, approximately 40% of smart phones users do not put passwords on their cell phones, through which they access vital organization/personal data and information (CISCO, 2013).

VI.2 Unreliable Information Security Policy

Information security policy can be defined as roles and responsibilities of employees to protect information system and technological resources of their organizations (Bulgurcu, Cavusoglu, & Benbasat, 2010). These policies are implemented to help employees to properly manage technological resources and managers of the organizations should help employee to follow these policies (Watters & Ziegler, 2016). Mostly, organizations adopt/creates IS security policies for the sake of compliance to international standards or governments, hence these policies fail to provide reliable security as they only remains in documents and not being practise(Hina & Dominic, 2018). Management fails to inforce policies to users and provide them with appropriate knowledge and regular training to equip them with reliable tools and knowledge about organizations IS security.

VI.3 Work Environment

In this paper, work environment is referred to as social features and physical conditions in which ICT users perform their jobs which includes management support, organization security culture and workload. Management support, is defined as the perceptions of employee's regarding management support and understanding of information system security in an organization. Management failure to motivate employee feeling of responsibility and ownership in decision about securityresults into increase in chances for IS security risks(Greene, 2010; Humaidi & Balakrishnan, 2015). Senior managers should be an example in the organization by insuring proper training and awareness programs and setting example to juniors while grooming their security behaviour (AlHogail, 2015,; W.D.Kearney & H.A.Kruger, 2016). Management failure to provide incentive to those who complies to the security policy increases organization's IS security risks (Padayachee, 2012; Predd, Pfleeger, Hunker, & Bulford, 2010; Hassan, Ismail, & Maarop, 2015).

Organization security culture, it involves establishment of policies, standards, training and education programs (Alhogail, Areej; Mirza, A., 2014). Communication, security policy, and organization structure are most mentioned information security factors by researchers (Safa, et al., 2015). Failure to motivate security culture within an organization by making people aware of various security issues, providing them with appropriate tools to react and two-way communication between technicians, managers and employees contribute to IS security risks.(AlHogail, 2015,; Alhogail, Areej; Mirza, A., 2014; Brock & Khan, 2017). Organization security culture supposed to be a long-term program, also not just a technical issue but a managerial issue as well.

Workload, in this study workload is refers as employees perception about the amount of work that need to be completed. Majority of violation of information security contributed to the employee behaviour of optimizing work by using optimum resources (Arian, Kusedghi, Raahemi, & Akbari, 2017). The pressure applied by organization to the staffs to achieve higher financial commitment and goals is an attribute to the ground of security violation (Martin, Rice, & Martin, 2016). Persistence pressure to perform work often resulted to employees taking risk to respond to the pressure (Allam, Flowerday, & Flowerday, 2014). Hence, management behaviour of evaluating workload and pressure employee into reaching impossible goals, results into employee finding solution from optimization applications that might not be reliable and become a source of IS security risks.

Internet and network, this refers to organization dependence on internet and network on daily activities. Connection to the internet is no longer a choice by today's organizations, rather a strategy to stay in the competitive market(Khan, Musa & Alshare, 2015; Saunders & Brynjolfsson, 2016). Thus, user need to be given more privilege to perform their work efficiently with consideration to the level of access. Maintaining a good level of security while using internet and network services require considerable amount of fund and resources, many organizations do not set aside funds for the matter(Brock & Khan, 2017; Al-Omari, El-Gayar, & Deokar, 2012). In organization where many systems are used, different privilege access have to be used like usernames and passwords, failure to restrict information based on levels will cause internal or external information breach (Etezady, 2011). Failure to restrict userfrom different level of access such as websites and installing of malicious software will riskorganization security. Also, failure to restrict user from uninstalling of necessary

software that keep internet security and virus software up to date in all computers over the network will open organization IS security to various threats(Connolly, Lang, & Tygar, 2014).

VI.4 Demographic Factor

This section describe the impacts of various demographic factors on information system security. Based on the research conducted by Barlow, Warkentin, Ormond and Dennis (2013) the factors like gender, age, education level, experience, computer usage, job title (position) and managerial role can be used as variables in predicting intention to comply with IS security. Different view represented by different researchers on the impact of demographic factors on compliance of IS security(Parsons, Kathryn; McCormac, Agata; Butavicius, Marcus; Pattinson, Malcolm; Jerram, Cate, 2014). Ferdani and Hovav (2014) prove that, age has strong impact on intention of employees to comply with IS security. However, in most cases, despite other many factors that contribute to violation of IS security, education level and knowledge on the information security to both genders, perceived to be a pivotal factor (Bulgurcu, Cavusoglu, & Benbasat, 2010; Parsons, Kathryn; McCormac, Agata; Butavicius, Marcus; Pattinson, Malcolm; Jerram, Cate, 2014). Lack of knowledge from both managers and employees, will open doors to IS security risks from within and outside the organization.

VII. CONCLUSION

The effort made by this paper is synthesizing literature to determine the most important/crucial factors against IS security so that to help modern computer users and organization in saving their limited resources and time on other factors. By answering the research question 1 on why IS security is still a disaster and research question 2 on what are the key factors that affect IS security. This study found that, numerous factors contribute to poor IS security management in organization depends on the ICT nature and security management culture of the organization (Parsons, McCormac, Butavicius, & Ferguson, 2010). However, the most common factors that affect the security of information system includes; human factorwhich includes trust and perceived privacy. Information security policies, which includes policy scope. Work environment aspects, which includes management support, organization security culture, work load and Internet and network usage. Lastly is demographic factor, which includes factors based on gender, age, education level, work experience, managerial role, job title and percentage of computer usage (Khan & AlShare, 2019).

Poor understanding of these key factors of IS security has resulted into continuous information security risk to both individuals of modern computer users and organizations. Furthermore, all factors identified in this paper as the key factors in IS security, they all seem to have one common and very important attribute, which is education/training/knowledge. Thus the paper propose the solution of utilizing social technical theory by providing employees with appropriate training that will help in changing their beliefs and norms that can change their perception of organization IS security. Appropriate and regular training can help in changing employees trust and sense of privacy about IS security. Knowledge about information security policy will help in insuring these policies are being respected and adhered. Understanding how various work environment situations can affect information system security will help both managers and employees in securing IS security. Also, knowledge on how gender can be contributing factor to information security system. Thus, understanding of all these factors and providing appropriate and regular trainings and awareness programs to both managers and users will help in strengthen organization IS security and get rid of security risk that keep on raging in organizations, particularly in Africa context.

REFERENCES

[1]. AlHogail, A. (2015,). Design and validation of information security culture framework. *Computers in Human Behavior, 49*, 567-575.

[2]. 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.

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

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

[5]. Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). Security Policy Compliance: User Acceptance Perspective. *IEEE, 45*(12), 1-10.

[6]. Arbanas, K., & Hrustek, N. Ž. (2019). Key Success Factors of Information Systems Security. *Journal of Information and Organizational Sciences, 43*(3), 131-144.

[7]. 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.

[8]. Astakhova, L. V. (2016). The ontological status of trust in information security. *Scientific and Technical Information Processing, 43*(1), 58-65.

[9]. 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.

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

[11]. 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.

[12]. Charitoudi, K., & Blyth, A. (2013). A Socio-Technical Approach to Cyber Risk Management and Impact Assessment. *Journal of Information Security, 4*(1), 33-41.

[13]. Chen, X., Chen, L., & Wu, D. (2011). Factors That Influence Employees' Security Policy Compliance: An Awareness-Motivation-Capability Perspective. *Journal of Computer Information Systems, 58*(4), 1-13.

[14]. CISCO. (2013). *BYOD Insights 2013: A Cisco Partner Network Study.* sunfrancisco : VAR Insight.

[15]. 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.

[16]. 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: 2do Congreso Nacional de Ingeniería Informática / Sistemas de Información (CoNaIISI).

[17]. Etezady, N. (2011). The Impact of ERP Investments on Organizational Performance. *International Journal of the Academic Business World, 5*(2), 27-33.

[18]. Fields, Z., Fields, Z., & Patrick, H. (2016). Security-Information Flow in the South African Public Sector. *Journal of Information Warfare, 15*(4), 68-85.

[19]. Glaspie, H. W., & Karwowski, W. (2018). Human Factors in Information SecurityCulture: A Literature Review. *Advances in Intelligent Systems and Computing*, 269-281.

[20]. 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.

[21]. 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: Fifth Annual Symposium on Information Assurance.

[22]. Han, D., Dai, Y., Tianlin Han, & Dai, X. (2015). Explore Awareness of Information Security: Insights from Cognitive Neuromechanism. *Computational Inteligence and NeuroCience* , 1-11.

[23]. Hassan, N. H., Ismail, Z., & Maarop, N. (2015). Information Security Culture, A systematic Literature Review. *he 5th International Conference on Computing and Informatics* (pp. 456-463). instanbul: he 5th International Conference on Computing and Informatics.

[24]. Helpnetsecurity. (2020). *445 million attacks detected since the beginning of 2020, COVID-19 wreaks havoc.* New York: Helpnetsecurity.

[25]. 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.

[26]. 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.

[27]. 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.

[28]. IBM Cost of Data Breach Report. (2020). *Cost of Data Breach Report.* New York: IBM.

[29]. ITU. (2017). *Global Cybersecurity Index (GCI).* Geneva, Switzerland: International Telecommunication Union.

[30]. 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.

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

[32]. LIFARS. (2020). *Impact of Data Breaches on Businesses Reputation and How to Minimize Risk.* New York: lifars.com cyber security solutions.

[33]. Lin, K.-M. (2016). Understanding undergraduates' problems from determinants of Facebook continuance intention. *Behaviour & Information Technology, 35*(9), 693-705.

[34]. Lubua, E. W., & Pretorius, P. D. (2019). Ranking Cybercrimes based on their impact to organisations' welfare. *THREAT Conference Proceedings* (pp. 1-11). Johannesburg: THREAT Conference Proceedings.

[35]. Lundgren, B., & Möller, N. (2017). Defining Information Security. *Science and Engineering Ethics, 25*(3), 1-8.

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

[37]. 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.

[38]. 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.

[39]. Metivier, B. (2017, April 17). *Sage Advice - Cybersecurity Blog*. Retrieved from Tyler Cybersecurity: 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

[40]. 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.

[41]. 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,.

[42]. Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Scuverse Science Direct* , 1-8.

[43]. 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.

[44]. Parsons, Kathryn; McCormac, Agata; Butavicius, Marcus; Pattinson, Malcolm; Jerram, Cate. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165-176.

[45]. Predd, J., Pfleeger, S. L., Hunker, J., & Bulford, C. (2010). Insiders Behaving Badly. *IEEE Security & Privacy, 6*(4).

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

[47]. Safa, N. S., khaka, M. S., Solms, R. V., Furnell, S., Ghani, N. A., & tHerawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security, 53*, 65-78.

[48]. Sapronov, K. (2020). The human factor and information security. *Kaspersky* .

[49]. Saunders, A., & Brynjolfsson, E. (2016). Valuing Information Technology Related Intangible Assets. *MIS Quarterly, 40*(1), 50-110.
[50]. Sausalito, C. (2020). *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*. New York: Cybercrimme Magazine.
[51]. 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.
[52]. 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.
[53]. URT. (2020). *Tanzania Budget Speach 2020/2021*. Dar es Salaam: The Citizen.
[54]. W.D.Kearney, & H.A.Kruger. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation? *Computers & Security, 61*, 46-58.
[55]. Watters, P. A., & Ziegler, J. (2016). Controlling information behaviour: the case for access control. *Behaviour & Information Technology, 35*(4), 268-276.
[56]. 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: 4th International Workshop on Socio-Technical Perspective in IS development (STPIS'18).

Adam A. Semlambo, et. al. " Factors Affecting the Security of Information Systems: A Literature Review." *The International Journal of Engineering and Science (IJES)*, 10(11), (2021): pp. 21-29.