Sep 15th, 2:00 PM - 2:30 PM

Determinants that affect information security awareness and behavior: A systematic literature review

Abdurehman Ali
Addis Ababa University, alliendalkachew@gmail.com

Solomon Negash
Kennesaw State University, snegash@yahoo.com

Determinants that affect information security awareness and behavior: A systematic literature review

Research Paper

Abdurehman Ali
Addis Ababa University
alliendalkachew@gmail.com

Solomon Negash
Kennesaw State University
snegash@yahoo.com

ABSTRACT

In today's digital age, it is crucial for all organizations to manage their information systems security. This makes them potentially endangered by actions of employees and users. So there is a need of investing more on security related issues; one of them is giving attention for the human i.e. the social aspect of security. This paper critically analysis the different literatures using a systematic literature review technique using PRISMA search protocol concerning the determinants which most affect information security awareness and behavior. The information security training or education has given more emphasis than behavior and attitude. Then after identifying those determinants, it filters out the areas further study is needed which includes information security knowledge and care. It is determined that employee information security awareness and conduct are highly influenced by information security training, attitude, and behavior. Due to the choice of search criteria and/or databases, some pertinent papers may not have been included in this literature review so as to the study focus on developing nations. The factors that affect employees' information security tasks and initiatives must be determined for future study.

Keywords

Information security, Information security awareness, Information security behavior.

INTRODUCTION

Today emerging of new technologies and information load are increasing. Information security is a preserving of information or systems from illegal use, access and damage (CNSS, 2010). Information security is a mechanism to protect organizations information technology assets against any incidents or breaches. Availability, confidentiality and integrity are the three properties of the basis of information security (Bishop, 2003). Information security management consists of the human (i.e. social) and technical features (Milov et al., 2022). This study focuses on human aspect of information security

awareness and behavior. It has three ways of delivering through training reward, campaign and punishment. The need of knowing information security awareness and behavioral issues is used for employees and senior managers for decision making in the organizations.

Currently, ensuring the information security is the priority task for any organization to guarantee information security management, first there is a need of information security awareness (Albrechtsen & Hovden, 2010) and the behavior of the individuals whether the threat comes from employees (insiders) or outsiders (Sommestand et al., 2013). Insider threat is a threat posed by employees or users who have access to the system of the organization and creates danger through hijacking their privileges (Theoharidou et al., 2005).

A number of studies have been conducted on this area but have limitations on identifying and stating the most influential determinants that affect employees' information security awareness and behaviors. This critical analysis covered 22 publications selected by following the systematic literature review techniques.

The outline of this paper analysis covered the introduction, the description on how the systematic review was performed, the body of knowledge (discussions) and finally the conclusion. This systematic literature review was about to identify the determinants (which was tested previously) that most influence employees information security awareness and behavior. Therefore, the research question was: *What are the determinants that affect information security awareness and behavior?*

Hansch and Benenson (2014) define information security awareness, based on different literatures; awareness as perception, protection and behavior. Security awareness as a behavior deals with in minimizing security incidents (breaches) and failures. So the focus is not in having the needed knowledge but the necessity is on security behavior.

Current trends show that as technological applications grow, so do the incidents (Valentine, 2006). Therefore, it is necessary to set up security policies. Many firms place less focus on making sure that user or employees are aware of incidents or threats. Security threats change along with new technologies and operating systems.

The study is important because different nations, especially those with low incomes, have made fewer investments in security issues because they are more concerned with how to use those systems that is why the study is focused on developing nation's context. As a result, they are not paying enough attention to how the system is vulnerable to insider threats because their main concern is connecting their organizations' systems online. The organizations vulnerability is increasing as those systems are dependent on employees who operate the systems. Many low income countries have less infrastructure establishment when considering their information system level. There are other threats due to less skilled labor as well (Karokola & Yngstrom, 2009). The low income countries especially the African countries organizations have lack of information security awareness and a well established strategic plan (Abu Musa, 2010).

METHODOLOGY

Literature search

In using systematic literature review the search process had a big impact on collecting the best and qualified publications in that field (Brocke et al., 2009). A set of procedures and guidelines should be

followed to ensure the qualities of the retrieved literatures to fulfill reliability and validity. The validity performed when searching the literatures by collecting the needed materials from databases and journals. Most of the literatures are from the international Information System journals but also from specific security and related journals and conference papers. These are selected because most of the articles concerning developing nation and information security related topics are found a lot.

Here are some of the lists from where the literatures were collected:

Academic Databases

- Elsevier Science Direct
- Institute of Electrical and Electronics Engineers (IEEE)
- Scopus

International Information Systems Journals

- International Journal of Science and Engineering Applications
- International Journal of Engineering and Advanced Technology
- Journal of Information Science
- Education and Information Technologies
- International Journal of Advanced Computer Science and Applications
- Association for Information Systems journals

Specialized Information Security Journals

- Computers and Security

Conference proceedings

- International Conference on Information Systems
- Information Systems International Conferences

Literature analysis

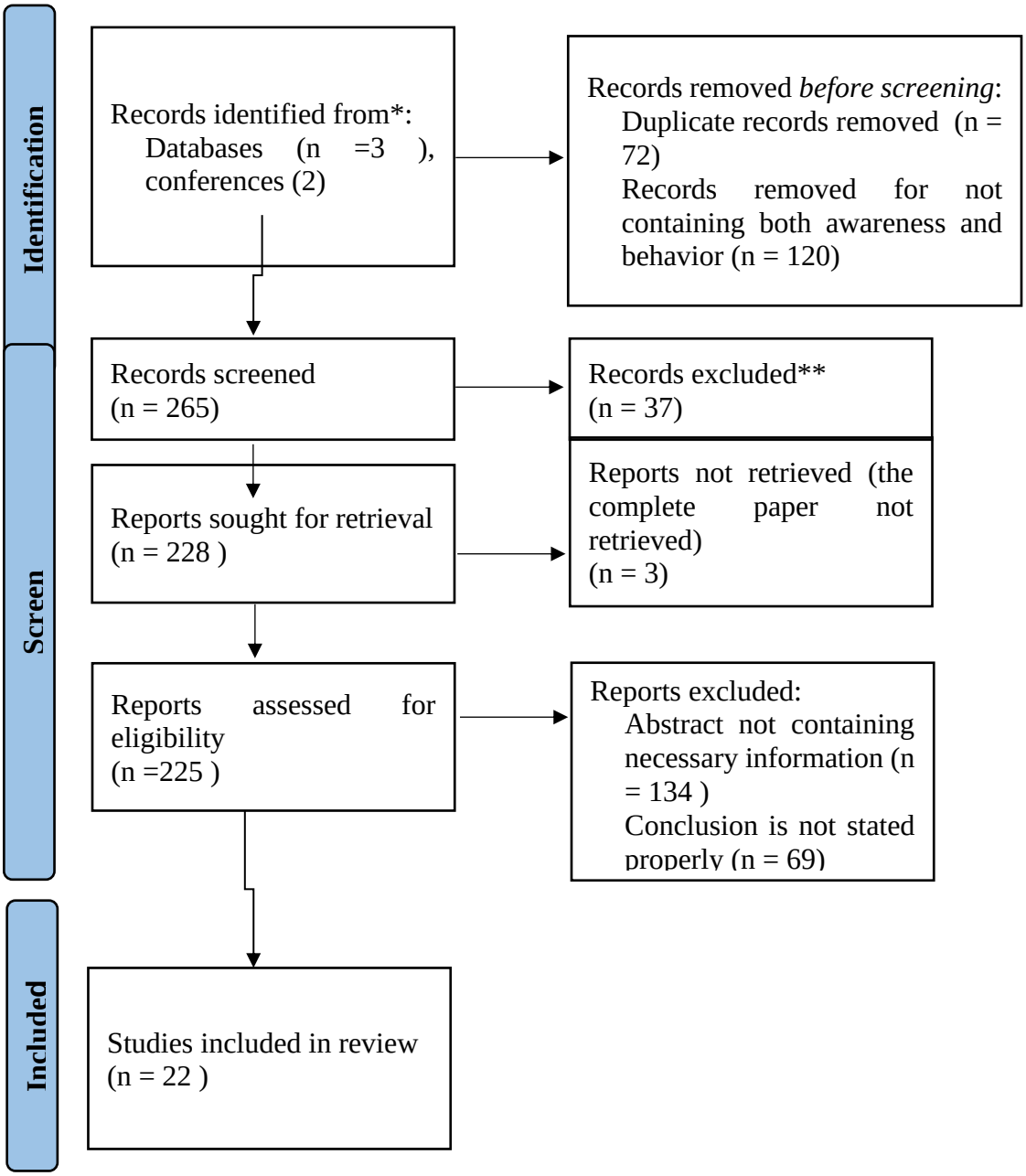
The first search process resulted in 457 potential literatures. In the next step, those publications were screened using concerning information security awareness and behavioral issues. The topics, titles, abstracts, conclusions if needed sometimes the whole write up was scanned and the publications within 16 years period included and for the searching process the following keywords were used.

Table1. *Keywords used for inclusion and exclusion criteria*

No	Phrase
1	(employees OR insiders OR users OR staffs) AND (information security awareness OR security awareness)
2	(employees OR insiders OR users OR staffs) AND (information security behaviors OR security behaviors)

By assessing the contents of the papers 225 articles were remaining, then further reduced to 22 to identify the determinants or constructs easily by focusing on specific literatures using both keywords (awareness and behavior) and focusing on articles which used mainly quantitative method (empirical study). Most of the articles were found from the known international databases (from Science Direct 6 Articles), Scopus (6), journals (9 Articles) and conferences (2 Articles) were filtered.

Table2. *Searching of refined papers for information security awareness and behavior using PRISMA diagram*



MOSTLY USED DETERMINANTS OF INFORMATION SECURITY AWARENESS AND BEHAVIOR

Technology usage becomes our day to day life; it is obvious that incidents will exist. The information security incidents and breaches are seriously increasing. For example in 2014/15 financial year 38% information security incidents were occurred (McCormac, 2017). This shows that employees were less aware of the information security and behaves not at a needed level.

Many studies conducted on human behavior of information security aspect like awareness and behavior (Puhakainen, 2006). Amazingly, over 80% of these come from its own organization due to weak policy and guidelines or staff awareness training (Hinde, 2002). There is a need of critically analyzed those determinants which have more influence in these aspects.

Different researches were conducted on how to improve the employees' information security awareness and behavior e.g. Training can improve the performance of the organization if employees are aware or behave the information security issues (Albrechtsen & Hovden, 2010). The employees' behavior needs to be assessed through information security awareness context.

Most of the time, employees of the organizations are not reporting the security incidents if it arises from inside, so they are fear the coming punishments from top managers (Herath & Rao, 2009). And also some employees are careless to report such incidents to the organizations and some are don't have a knowhow on how to conduct a report (Colwill, 2010).

To increase information security performance, there is a need of information security training (Albrechtsen & Hovden, 2010) which was conducted using intervention study and had impact only at the individual level. But it needs to integrate other determinants to include organizational level characteristics.

The relationship between individual information security awareness and individual difference determinants examined (McCormac, 2016). But when doing this the data was collected using self-report method, this can create data bias. After assessing these determinants, one can do future research which will focus on information security awareness as a part of organizational security strategy or information security management task.

The influence of information security behavior specifically studied with Brazilian users and added a new determinant (i.e. satisfaction) to information security field (Klein & Luciano, 2016). They had limitations on showing the behavioral information security issues which are more culture based but the chances of variance between different countries is not highly articulated.

The effectiveness of information security awareness gained through campaign based on psychological theories of awareness and behavior measured in organizations (Khan et al., 2011). Others state the main determinants that influence information security behavior to increasing awareness and ability of professionals (Bojmaeh, 2015). Thus, for leading to information security management issues there is a need of incorporating other determinants or determinants with the studies in order to be the R-square value higher which measures the significance.

The information technology as safeguarding measure, the behaviors of personal computer users explored (Liang & Xue, 2010) by suggesting a new model with the source basically focuses on the technology. But no work is done on integrating the different sources like person or event. So there is a need of adding other determinants which encircles these issues.

Table 3*. Lists of mostly used determinants in each different studies*

Author(s) of the study	Study title	Major Determinants used
(Karjalainen, Siponen & Sarker, 2020)	Toward a stage theory of the development of employees' information security behavior	Intuitive thinking Declarative thinking

Author(s) of the study	Study title	Major Determinants used
		Agency-related thinking
		Routine-related thinking
(Haeussinger & Kranz, 2013)	Information security awareness: its antecedents and mediating effects on security compliant behavior	Institutional antecedents
		Information security policy provision
		Security education training awareness (SETA)
		Individual antecedents
		Information security knowledge
		-negative experience
		Environmental antecedents
		-peer behavior
		-security source behavior
(Bojmaeh, 2015)	The main determinants influencing information security behavior	Self-efficacy
		Intention to Information Technology security practice
		Security practice care behavior
		Security practice technology
(Mishra et al., 2014)	Information security behavioral model: towards employees knowledge and attitude	Knowledge
		Attitude
		Behavior
(Bauer, Bernroider & Chudzikowski, 2017)	Prevention is better than cure! Designing	IS risks
	information security awareness programs to	Responsibilities,
	overcome users' non-compliance with information	ISP importance
	security policies in banks	Knowledge
		Neutralization behaviors
(Alkhazi, Alshaikh, Alkhezi & Labbaci, 2022)	Assessment of the Impact of Information Security	Text-based training
	Awareness Training Methods on Knowledge,	Game-based training
	Attitude, and Behavior	Self-education activities
		Intervention strategy

Author(s) of the study	Study title	Major Determinants used
(Albayrak & Bagci, 2022)	Modelling the effects of personal determinants on information security awareness	Technology attitude Information security training Department
(Hong, Chi, Liu, Zhang, Lei & Xu, 2023)	The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates	Knowledge Attitude Behavior
(Al-Shanfari, Yassin, Tabook, Ismail & Ismail, 2022)	Determinants of Information Security Awareness and Behaviour Strategies in Public Sector Organizations among Employees	Determinants from (Protection Motivation Theory, the Theory of Planned Behaviour, the General Deterrence Theory) Facilitating Conditions
(Klein & Luciano, 2016)	What influence information security behavior? A study with Brazilian users	Safe behavior -threat susceptibility -threat severity -certainty of detection -punishment severity -satisfaction -safeguard effort
(McCormac, 2017)	Individual differences and information security awareness	Conscientiousness Agreeableness Emotional stability Risk taking propensity
(Semlambo, Mkude & Lubua, 2021)	Determinants Affecting the Security of Information Systems: A Literature Review	Human determinant (trust and perceived privacy) Information security policies, (policy and scope) Work environment (management support, organization security

Author(s) of the study	Study title	Major Determinants used
		culture, work load, Internet and network usage) Demographic determinant (gender, age, education level, work experience, managerial role, job title and percentage of computer usage)
(Ahlan, Lubis & Lubis, 2015)	Information security awareness at the knowledge-based institution: its antecedents and measures	Self-attitude Intention to comply Perceived threats Social pressure Self-behavior Policy compliance Info. security awareness Self-cognitive Training program Peer performance Religious indicator
(Al-Shanfari, Abdullah & Mohamed, 2020)	Identify of Determinants Affecting Information Security Awareness and Weight Analysis Process	Constructs of PMT and TPB are the most utilized determinants
Klein & Luciano, 2016)	What influences information security behavior? A study with Brazilian users	Human perception of: Threat Control Disgruntlement
(Cheng Li, Li, Holm & Zhai, 2013)	Understand the violation of Information System security policy in organizations: an integrated model based on social control and deterrence theory	Security behavior Security awareness

Author(s) of the study	Study title	Major Determinants used
(Wiley, McCormac & Calic, 2020)	More than the individual: Examining the relationship between culture and Information Security Awareness	ISA, organisational culture, and security culture
(Hassandoust, & Techatassanasoontorn, 2020)	Understanding users' information security awareness and intentions	Security education, training and awareness (SETA) programme, countermeasures awareness, the role of InfoSec awareness, coping and threat appraisals.
(Limna, Kraiwanit & Siripipattanakul, 2022)	The Relationship between Cyber Security Awareness, Knowledge, and Behavioural Choice Protection among Mobile Banking Users in Thailand	Cybersecurity awareness, behavioural choice protection, security knowledge and behavioural choice protection.
(Candiwan, Azmi & Alamsyah, 2022).	Analysis of Behavioral and Information Security Awareness among Users of Zoom Application in COVID-19 Era	Demographics, Daily Internet usage time
(Sasse, Hielscher, Friedauer & Buckmann, 2022)	Rebooting IT Security Awareness – How Organisations Can Encourage and Sustain Secure Behaviours	Security Behaviour Curve – concordance, self-efficacy, and embedding
(Yerby & Floyd, 2018)	Faculty and staff information security awareness and behaviors	Comprehensive security awareness training

The first four most used determinants were:

1. Information security training (7 studies)
2. Attitude (5 studies)
3. Behavior (5 studies)
4. Security practice care, self-efficacy, knowledge and security awareness (each in 2 studies)

As we can see from the above table, most of the determinants are the constructs of those behavioral models which are more focused on human aspect of the study. These constructs are components of mostly the two theories, theory of planned behavior (TPB), protection motivation theory (PMT). These theories originally developed from management and psychology fields.

According to Puhakainen (2006) constructed a three design theories for information system security awareness namely training reward, punishment and campaign to change attitude and information security behavior. But as shown from the literatures, only the determinants of those known theories are assessed repeatedly and other needed determinants are not taken into account. Most of the awareness studies are focused on Security Educational Training Awareness (SETA) giving less attention for the other approaches of campaign, reward and punishment. So the determinants of other behavioral study theories like health protection behavior (HPB) theory for careful behavior among employees' influenced by perceptions related to threat, theory of reasoned action should be addressed well for future research.

DISCUSSION AND CONCLUSION

The existing literatures were systematically analyzed with the purpose of analyzing those papers with the type of information security management specifically information security awareness and behavior. This critical paper analysis showed that information security awareness is a starting point to secure the information of any organization and to behave accordingly. There is a need of creating security awareness issues among employees & the community as a whole and need of investigating employees' behavior towards information security and how they are aware of information security.

Educational training is explored through the aid of action research resembles information system security campaigns through deploying the convergence model of communication. Therefore, there is a need of exploring new constructs which consists the basis of convergence model use for information security awareness campaign approach.

There are so many determinants which are incorporated from different theories (including other disciplines) for information security awareness & behavior and more for the purpose of educational training area. Hence, there is a need of more emphases should be given for campaign, punishment & reward areas and also emphasis should be given for behavior related theories and for their determinants as indicated from the table like perceived severity like security violation, perceived likelihood (security breach) which both related to perception security threat for protection.

According to the results of the research, employees' awareness of and behavior toward information security is significantly influenced by information security training, attitude, and behavior. The study's findings indicated that additional research should be done on coping, threat assessments, daily internet usage, curve-concordance, and embedding, while frequent training programs should be conducted to gauge employee comprehension of security regulations.

Research limitations and implications - Because of the choice of search terms and/or databases, some pertinent papers may not have been included in this literature evaluation. Practical ramifications - This study provides an overview of factors that have been shown to affect workers' awareness and conduct. As a result, concrete information security training measures are possible. Finding the factors that affect employees' information security tasks, initiatives, challenges, and opinions on them is required to develop this study. Future research may examine how different models and individual factors affect how information security knowledge and behavior are implemented.

REFERENCES

Abu-Musa, A. (2010). Information security governance in Saudi organizations: an empirical study, Information Management & Computer Security, 18(4), pp.226-276.

Ahlan, A. R., Lubis, M., & Lubis, A. R. (2015). Information security awareness at the knowledge-based institution: its antecedents and measures. Procedia Computer Science, 72, 361-373.

Albayrak, E., & Bağcı, H. (2022). Modelling the effects of personal factors on information security awareness. Journal of Information Science, 01655515221127609.

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Computers & Security, 29(4), 432-445.

Alkhazi, B., Alshaikh, M., Alkhezi, S., & Labbaci, H. (2022). Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior. IEEE Access, 10, 132132-132143.

Al-Shanfari, I., Yassin, W., Tabook, N., Ismail, R., & Ismail, A. (2022). Determinants of Information Security Awareness and Behaviour Strategies in Public Sector Organizations among Employees. International Journal of Advanced Computer Science and Applications (IJACSA).

Al-Shanfari, I., Yassin, W., & Abdullah, R. (2020). Identify of factors affecting information security awareness and weight analysis Process. International Journal of Engineering and Advanced Technology (IJEAT), 9(3), 534-42.

Bauer, S., Bernroider, E. W., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. computers & security, 68, 145-159.

Bishop, M. (2003). Computer security: Art and science. 2003. Westford, MA: Addison Wesley Professional, 4-12.

Bojmaeh, H. (2015). The Main Determinants Influencing Information Security Behavior, International Journal of Science and Engineering Applications Volume 4 Issue 6, 2015, ISSN-2319-7560

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. MIS quarterly, 39(4), 837-864.

Brocke, V., Simons, J., Niehaves, A., Riemer, B., Plattfaut, K., & Cleven, A. (2009). Reconstructing The Giant: On the Importance of Rigour in Documenting the Literature Search Process, in Proceedings of the 17th European Conference on Information Systems (ECIS), Verona, Italy.

Candiwan, C., Azmi, M., & Alamsyah, A. (2022). Analysis of behavioral and information security awareness among users of zoom application in COVID-19 era. International Journal of Safety and Security Engineering, 12(2), 229-237.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. Computers & Security, 39, 447-459.

CNSS. (2010). National Information Assurance Glossary.

Colwill, C. (2010). Human determinants in information security-The insider threat – Who can you trust these days, Information Security technical Report 14, p.186-197.

Haeussinger, F., & Kranz, J. (2013). Information security awareness: Its antecedents and mediating effects on security compliant behavior.

Hansch, N., & Benenson, Z. (2014, September). Specifying IT security awareness. In 2014 25th International workshop on database and expert systems applications (pp. 326-330). IEEE.

Hassandoust, F., & Techatassanasoontorn, A. A. (2020). Understanding users' information security awareness and intentions: A full nomology of protection motivation theory. In Cyber influence and cognitive threats (pp. 129-143). Academic Press.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2), 154-165.

Hinde, S. (2002). Security surveys spring crop. Computers & Security, 21(4), 310-321.

Hong, W. C. H., Chi, C., Liu, J., Zhang, Y., Lei, V. N. L., & Xu, X. (2023). The influence of social education level on cybersecurity awareness and behaviour: A comparative study of university students and working graduates. Education and Information Technologies, 28(1), 439-470.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. MIS quarterly, 549-566.

Karjalainen, M., Siponen, M., & Sarker, S. (2020). Toward a stage theory of the development of employees' information security behavior. Computers & Security, 93, 101782.

Karokola, G. & Yngström, L. (2008). Lessons Learnt in the Process of Computerization, Automation and Management of ICT Security in the Developing World: A Case Study of the University of Dar Es Salaam, Tanzania, Proceedings of the ISSA 2008 – Innovative Minds Conference. Gauteng Region (Johannesburg), South Africa.

Karokola, G., & Yngström, L. (2009). State of e-Government Development in the Developing World: Case of Tanzania-Security vie. In 5th International Conference on e-Government (pp. 92-100). ACADEMIC CONFERENCES LTD.

Khan, B., Alghathbar, K. & Khan, M. (2011). Effectiveness of information security awareness

methods based on psychological theories, African Journal of Business Management Vol. 5(26), pp. 10862-10868.

Klein, R. H., & Luciano, E. M. (2016). What influences information security behavior? A study with Brazilian users. JISTEM-Journal of Information Systems and Technology Management, 13, 479-496.

Liang, H., & Xue, Y. L. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. Journal of the association for information systems, 11(7), 1.

Limna, P., Kraiwanit, T., & Siripipattanakul, S. (2022). The Relationship between Cyber Security Awareness, Knowledge, and Behavioural Choice Protection among Mobile Banking Users in Thailand. International Journal Of Computing Sciences Research, 6, 1-19.

Lubua, E. W., Semlambo, A. A., & Mkude, C. G. (2022). Factors Affecting the Security of Information Systems in Africa: A Literature Review. University of Dar es Salaam Library Journal, 17(2), 94-114.

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

Milov, O., Khvostenko, V., Natalia, V., Korol, O., & Zviertseva, N. (2022, June). Situational Control of Cyber Security in Socio-Cyber-Physical Systems. In 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (pp. 1-6). IEEE.

Mishra, S., Snehlata, S., & Srivastava, A. (2014). Information Security Behavioral Model: Towards Employees' Knowledge and Attitude. Journal of Telematics and Informatics, 2(1), 22-28.

NIST. (1998). Information technology security training requirements: a role and performance-based model.

Puhakainen, P. (2006). A Design Theory for Information Security Awareness, Ph.D. Thesis. Department Information Processing Science.

Sasse, M. A., Hielscher, J., Friedauer, J., & Buckmann, A. (2022, September). Rebooting IT Security Awareness–How Organisations Can Encourage and Sustain Secure Behaviours. In European Symposium on Research in Computer Security (pp. 248-265). Cham: Springer International Publishing.

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. Information Management & Computer Security, 22(1), 42-75.

Theoharidou, M., Kokolakis, S., Karyda, M. & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799, Computers and Security, vol. 24(6), pp. 473- 484.

Valentine, J. A. (2006). Enhancing the employee security awareness model. Computer fraud & security, 2006(6), 17-19.

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. Computers & security, 88, 101640.

Yerby, J., & Floyd, K. (2018, August). Faculty and staff information security awareness and behaviors. In Journal of The Colloquium for Information Systems Security Education (Vol. 6, No. 1, pp. 23-23).