ISSN(Online) : *2456-8910*
International Journal of Innovative Research in Applied Sciences and Engineering (IJIRASE)
Volume 4, Issue 9, DOI:10.29027/IJIRASE.v4.i9.2021.905-912,March 2021

Investigating the Level of Awareness on Information Security Amongst Users at Botho University

Kabelo Mbereki [1], Srinath Doss [2]
[1]Post Graduate Student, Botho University, Gaborone, Botswana
[2]Fellow , Faculty of Computing, Botho University, Gaborone, Botswana

Email: kabelo.mbereki@bothouniversity.ac.bw, srinath.doss@bothouniversity.ac.bw

Abstract: The growth of technology advancement has promoted a borderless environment among users, organizations, global industry and easy access to information. The use of the internet and computer systems in a teaching environment parallel increased the number of threats in today's world. Lack of information security practices are the major cause to security breaches. Information security needs to be addressed amongst users for the protection of organizational assets. Human knowledge, attitude and behaviors habitually influence information security. Humans are considered as the least strong link concerning information security. The study explores a literature review in information security awareness amongst users. As a result, this research will come up with a proposed security awareness framework to enforce information security practices

Keywords: Information Security, Awareness, security breaches, human knowledge, attitude, behaviour, threats.

I. Introduction

Info security is an essential aspect of technology worldwide. Organizational information assets are stored in electronic form and data processing through information technology that is transferred over private networks and the internet. Protection against information leaks is a challenge the IT industry is facing today. With technological advancement, different types of threats are emerging. With the increase in different types of threat, this has led to increased importance on information security concerns. Organizations often have security policies to act as a guide on how the organization manages and protects its assets. However, the IT industry's implementation of info security solutions is much into the technical part, often ignoring the human factor. Hence security is everyone's responsibility. The nature of the working environment in higher learning institutions where software and hardware availability is necessary to meet teaching and research goals, the protection of information can be difficult. It's evident that emerging technologies such as smartphones, networks, wireless, and computing devices have brought many benefits to the corporate world. Info security is essential for many organizations, especially with the introduction of the internet. Unplanned misconduct by end users can result in severe destruction such as loss of clients, loss of reputation and financial losses. Organizational information needs to be protected from unauthorized access.

II. Objectives

The research study aims to fulfill the following objectives;

1. To explore the effectiveness of info security policies towards information security awareness.
2. To assess info security practices amongst users.
3. To explore the role of info security training towards awareness of information security.
4. To assess the likelihood of threat that may result due to lack of awareness on information security.

5. To study user's knowledge, attitude and behavior about awareness on information security.

III. Methodology

a. Quantitative Research Method

The evaluation procedure presented in this study will focus on quantitative research. Crewell (2003) cited in Williams (2007) defined quantitative research as a collection of quantification data and subject to statistical to support alternative knowledge claims. Klazema (2014) noted that quantitative research focuses more on numerical data. Numerical data can be used for mathematical analyses to investigate what is being observed. Literature review indicates that quantitative research methods such as questionnaires and surveys have been fruitful in the information security study. A number of reasons have been considered by the researcher when choosing quantitative research. The study will be focusing on a large number of users for feedback; therefore, large sets of data will be involved to quantify these to draw conclusions. With such statistics, the analysis can be considered more reliable.

b. Data Collection Instruments

Data collections involve the process of gathering information for various purposes. In research perceptive, it can be defined as gathering information, analysing the variables in a systematic technique to answer research questions, and evaluating the findings. Types of data are classified into two categories, namely primary data and secondary data. Primary data denotes information gathered directly from first-hand sources through questionnaires, observation, and experiments and not subject to any manipulation. Secondary data refers to information collected by someone other than the researcher, such as published data, books, magazines, and journals. The researcher opted to gather primary data through the use of a questionnaire as a collection instrument. Questionnaires in this context are a necessary instrument for providing valuable facts regarding the level of awareness on information security. Secondary data has helped address the theoretical background of the study with regard to information security awareness. Sources such as books, the internet, journals and research studies have been helpful to support the subject.

c. Sampling

Bordens and Abbott (2011) defined sampling as the practice of choosing a particular number of participants from a defined population as representatives of that particular population. According to Dawson (2002) indicated that from the quantitative research perceptive, it is believed that if sampling is chosen correctly using the right procedure, it is then likely to take a broad view of the results to the entire research population. To clarify the two terms, sample and population, the researcher distinguishes the two terms in the following manner. A sample is the selection of subset of individuals from a larger population. According to Walliman (2011), the sampling procedure is categorized into two, namely, probability sampling and non-probability sampling. According to Kothari (2004), probability sampling is focused on the idea of random sampling, systematic sampling, cluster sampling and stratified sampling. Therefore, probability sampling is a raffle in which a subset of individuals is selected from the population using some mechanical process. The results attained from probability sampling would be assured in terms of probability. The researcher can measure the fault of evaluation or the importance of the results attained from probability sampling. According to Walliman (2011), the selection process should ensure that each individual in the population has an identical opportunity to be chosen.

d. Target Participants

Olsen (2012) described participation as the involvement of people or organization in a process facilitated by the researcher. As per the literature review, university staff and students are the common participants in theory-testing research, particularly on information security awareness. Participants involved both Botho University staff and students. Most of the participants had used information systems at certain times and were literate to understand the study instrument. To explore user's knowledge, behaviours and attitude towards information security, 700 participants were involved in the study, 250 were students and 150 members of the staff from the sample size. These participants are in different positions and different backgrounds. The objective was to get different opinions and perspectives from numerous users.

e. Data Analysis

Sources of data identified in this study include quantitative, which is the primary source of data. A quantitative approach was adopted to explore and examine the level of awareness of information amongst users. Data is analyzed to identify various factors that maximize the level of awareness of information security amongst users. Data collected through a primary survey was compiled and analyzed using a statistical package for social scientists as well as Microsoft excel. Data is scrutinized to remove non-responsive answers. The chapter includes descriptive statistics of the participant's characteristics. The participants features include; gender, age, qualification, field, department, position, and job-title.

f. Bias Elimination

According to Sarniak (2015) mentioned, eliminating bias is not to make everyone the same but to make sure that the questions are considerately modeled and distributed to allow participants to disclose their real states without distortions. Hence bias in research can cause misleading results and wrong conclusions. To guard against bias the researcher in this study has developed a questionnaire that uses unbiased wording, style and structure to get reliable results. The researcher designed the right questions relevant to this study. It's imperative for the researcher to target participants that fit the research goals, known as selection bias. Hence surveying the wrong people is completely avoided. According to the literature, review bias can be introduced when raw data is transformed into miscalculated findings. Inappropriate statistical techniques are often the cause that usually leads to incorrect analysis of the questionnaire results. To avoid this from happening, the researcher used a proper statistical test to interpret the results.

g. Ethical Consideration

R Hussey and Hussey (1997) cited in Ong (2015), states that caution needs to be taken with regard to moral and ethical issues for any research type. The researcher is much aware of the responsibility and respect for research participants taking part in the study. The researcher will thus ensure participants have given informed consent. Participants were given almost a week to complete a questionnaire prepared in goggle form and those questionnaires were sent through their emails. The researcher made it clear to the participants that the study is voluntary if, at any point, they are free to withdraw. Participant's privacy was respected and maintained at all times; everything they shared was treated as confidential. As a result, research participants were free from deception when taking part in this research.

IV. Technology Description

a. Information Security Overview

"Users are the heart of any security system" Matt Bishop

Many organizations make use of technology to store sensitive information that is used for business operations. Before exploring further, it is vital to define few terms that will be used in this context. A review of different sources of information technology terms has revealed numerous definitions. The committee of national security systems cited in Whitman and Mattord (2016) has defined information security as the practice of protecting information and its electronic devices, including the systems that store, and convey information. This means that a business will have a drawback if there is the harm in confidentiality, integrity and availability.

According to Panacea M and Srinath Doss (2017) mentioned, information security comprises people, organizational factors, technology, and the working environment. The technical approach in defending against attacks includes implementing firewalls, access controls, antivirus, authentication and intrusion detection systems. Such measure covers the security model, confidentiality, integrity and availability. Information system security is more technical with less attention on people (Koskosas and Asimopoulos 2011). Tapiwa (2012) mentioned that the connectivity among computer systems and resource sharing has led to intrusion and data theft escalation. Focusing on a technical approach is not enough; therefore, there is a need for human assessment for security matters. Rao and Nayak (2014) as quoted in Haeussinger (2015) states that information security is an endless practice that comprises individuals, procedures and technology. Information security has been scrutinized into three components, as illustrated in figure1.1 **(**Rao and Nayak 2014) (cited Haeussinger 2015). As shown in the below figure 1.1, people as part of information security components consist of computer users, which can be categorized as system administrators, students, and staff in this study.

People's information security component is characterized by an individual's knowledge, behaviour and skills (Lewis & Memon 2013) quoted by (Ong, 2015). Therefore information security threats from people side could be deliberately or unintentional. An organizational component of information security which includes policies and processes, indicates that policies are aimed to inform members of an organization of their mandatory responsibility in protecting organizational information (Lee, 2001). According to Mahabi (2010), corporate policies enforce proper actions within an organization to reduce the abuse of information. According to Wiant (2005) as cited in Mahabi (2010) (Alfred Moselekatsi and Srinath Doss, 2017), emphasized that security policy alone it's not enough; reasonably, it is a setup where a decision can be taken. Therefore policies and procedures must take people into account. The technology components focus much on the technical part of information security. These include the implementation of security software, firewall, intrusion detection system, and regular penetration tests.

V. Results

This chapter has presented data from students' perspectives as well as staff. Quantitative data analysis was achieved using SPSS and Microsoft excel. There were no missing data during coding and therefore, all the respondents' data were usable during data presentation. Results indicate that both staff and students are not aware of information security policies. Findings from both participants group (staff and students) show that users don't know how to protect themselves from security threats such as pharming, phishing and social engineering. The next chapter will discuss results interpretation, future research as well as the implication of the study.

b. Business Benefits

As organizations expand the technology advancement and train their IT personnel, nothing much is done to accelerate awareness of system users' information security, hence making users the weakest linkage in information security. In today's world, cybercriminals are putting more effort into exploring and developing innovative hacking techniques to breach an organization's IT security (Aloul, 2012) and (Baboloki Janet and Srinath Doss,2017).Many organizations have invested much into technical aspects such as intrusion detections system, firewalls and many other technical controls; however, if the end-users are not informed and not following the security measures and practices mentioned in the policy, the legitimacy of security measures loss value. End-user behavior can cripple the organization finances, data loss and loss of repudiation. Such incidents need to be mitigated from the beginning. Therefore, the study's findings will assist Botho University IT managers in developing better plans in implementing user awareness and training programs (information security awareness framework). These will consequently help all Botho University stakeholders to have a better understanding of its policy on information security. Knowledge on information security awareness will help end-users about what to DO and what NOT to do when operating IT devices. Thus assisting the organization to achieve acceptable level of risk. Exploring a non-technical technique based on user's behavior will help the organization focus both on technical and non-technical approaches regarding information security. With the study focusing much on user's behaviour this will also help them appreciate their efforts or contribution towards keeping organizational information safe. In conclusion, with the above, an investigation on the level of awareness on information security will contribute to existing information security knowledge.

VI. Conclusions

a. Future research

New findings and recommendations are identified in this study to improve information security in Botho University. Further research is required to conduct the effectiveness of the recommended information security framework of this research. Moreover, future research should be inclusive of end-users interviews so that the researcher can get depth on information security practice. The research can also look into tertiary education in Botswana so that there can be a comparison of tertiary education results. Hence this comparison can provide a better understanding on information security awareness in an academic environment. Future research should use multiple survey methods to gather information about security awareness across a wide set of organizations. With the growth of technology at a high rate, a study on the relationship between gender, age and career are also significant for future research.

b. Recommendations

The recommendations presented here are meant to address, guide Botho University or any similar organizations on successfully operating and managing the information security awareness framework. The proposed solution address lack of information security awareness among users at Botho University is the development of an information security awareness framework. The information security awareness framework is developed to account for the targeted audience profile: Botho University staff and students. Questions such as what behavior we desire to and what knowledge or skills we want our audience acquire and apply are considering the framework development.

The proposed framework is presented in the below figure. The framework is composed of Information security policies, Risk assessment, auditing, information security awareness training and compliance. The framework also addresses people and security control to achieve risk reduction. As depicted in figure 24, Business objectives and security threats are the driving forces in the information security awareness framework. Therefore the framework must be aligned with information security threats along with the business objectives of the organization.

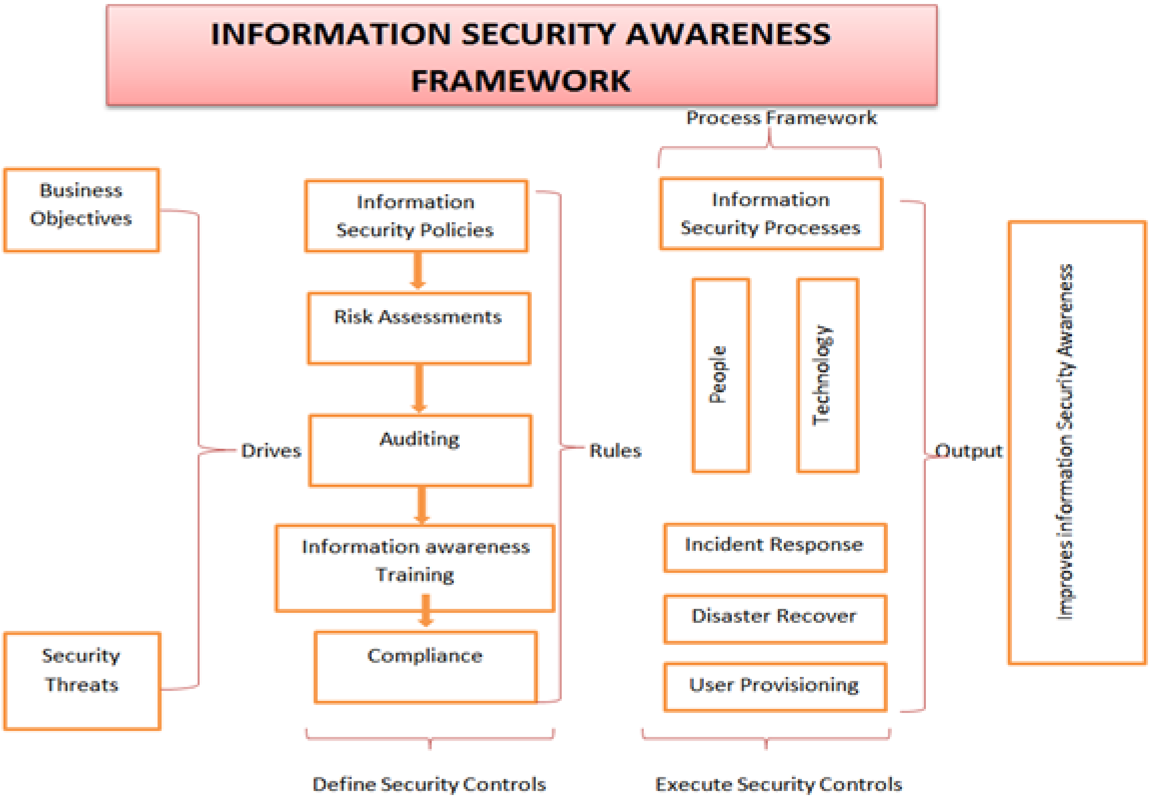
INFORMATION SECURITY AWARENESS FRAMEWORK
Process Framework
Business Objectives
Security Threats
Drives
Information Security Policies
Risk Assessments
Auditing
Information awareness Training
Compliance
Rules
Information Security Processes
People
Technology
Incident Response
Disaster Recover
User Provisioning
Output
Improves information Security Awareness
Define Security Controls
Execute Security Controls

Fig.1. Information security awareness framework

c. *Conclusion*

Technology is the driving force for information security. For information security awareness to be effective, it is supposed to be part of every individual within the organization. Or else, organizations will find themselves being exposed to information security gaps because they had little input to information security awareness. As already mentioned, with well-defined information security policy makes a successful security framework. This study has answered the research questions based on the questionnaire analysis from students and staff. Literature review was conducted and a study was designed to conduct quantitative research. The questionnaire analysis entailed 201 participants. The lesson learned in this study is that information security awareness is very critical to organizations. Through information security awareness training, end-users will gain more knowledge on security issues. Limitations of the research were discussed to give room more opening for upcoming research.

REFERENCES

[1]. A. Aloul, F. (2012). The Need for Effective Information Security Awareness. *JOURNAL OF ADVANCES IN INFORMATION TECHNOLOGY*, 3(3), pp.176-181.

[2]. Adéle Da Veiga, (2016) "Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study", *Information& Computer Security*, Vol. 24 Issue: 2, pp.139-151, https://doi.org/10.1108/ICS-12-2015-0048

[3]. Agarwal, D. and Garg, M. (2012). The Importance of Communication within Organizations: A Research on Two Hotels in Uttarakhand. *Journal of Business and Management (IOSRJBM)*, 3(2), pp.40-49.

[4]. Ahlan, A., Lubis, M. and Lubis, A. (2015). Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures. *Procedia Computer Science*, 72, pp.361-373

[5]. Alavi, R. (2016). *A Risk-Driven Investment Model for Analysing Human Factors in Information Security*. Ph.D. University of East London.

[6]. ALHOGAIL, A. and MIRZA, D. (2014). A FRAMEWORK OF INFORMATION SECURITY CULTURE CHANGE. *Journal of Theoretical and Applied Information Technology*, 64(2), pp.541-548.

[7]. Aliti, A. (2011). *Employees' Role in Improving Information Systems Security*. Masters. Linnaeus University.

[8]. Aloul, F. (2012). The Need for Effective Information Security Awareness. *JOURNAL OF ADVANCES IN INFORMATION TECHNOLOGY*, Vol 3(NO.3), p.1.

[9]. Al-Shehri, Y. (2012). Information Security Awareness and Culture. *British Journal of Arts and Social Sciences*, 6(1), pp.61-68.

[10]. Arachchilage, N. (2012). *Security Awareness of Computer Users: A Game Based Learning Approach*. Ph.D. Brunel University.

[11]. Arachchilage, N. (2012). *Security Awareness of Computer Users: A Game Based Learning Approach*. Ph.D. Brunel University.

[12]. Arizzi, R. (n.d.). *History of Information Security | Study.com*. [online] Study.com. Available at: http://study.com/academy/lesson/history-of-information-security.html [Accessed 23 Nov. 2017].

[13]. Banfield, J. (2016). *A Study of Information Security Awareness Program Effectiveness in Predicting End-User Security Behavior*. Ph.D. Eastern Michigan University.

[14]. Barua, A. (2013). METHODS FOR DECISION-MAKING IN SURVEY QUESTIONNAIRES BASED ON LIKERT SCALE. *Journal of Asian Scientific Research*, 3(1), pp.35-38.

[15]. Bilal Khan (2011). Effectiveness of information security awareness methods based on psychological theories. *AFRICAN JOURNAL OF BUSINESS MANAGEMENT*, 5(26).

[16]. Bird, D. (2009). The use of questionnaires for acquiring information on public perception of natural hazards and risk mitigation – a review of current knowledge and practice. *Natural Hazards and Earth System Sciences*.

[17]. Birmingham, P, & Wilkinson, D (2003). Using Research Instruments : A Guide for Researchers, Taylor and Francis, Abingdon, Oxon. Available from: ProQuestEbook Central. [11 September 2017].

[18]. Bishop, M. (2008). *Introduction to computer security*. Boston: Addison-Wesley, pp.35-36.

[19]. Bordens, K. and Abbott, B. (2011). *Research design and methods*. 8th ed. New York: McGraw-Hill, pp.261-262.

[20]. Chan, H. and Mubarak, S. (2012). Significance of Information Security Awareness in the Higher Education Sector. *International Journal of Computer Applications*, 60(10), pp.23-31.

[21]. Chang, A. (2015). *Theory of Planned Behavior & Smoking*. [online] LIVESTRONG.COM. Available at: http://www.livestrong.com/article/221185-theory-of-planned-behavior-smoking/ [Accessed 26 Jul. 2017].

[22]. Chen, C. C., Shaw, R. S., & Yang, S. C. (2006). MITIGATING INFORMATION SECURITY RISKS BY INCREASING USER SECURITY AWARENESS: A CASE STUDY OF AN INFORMATION SECURITY AWARENESS SYSTEM. *Information Technology, Learning, and Performance Journal*, *24*(1), 1-14. Retrieved from https://search.proquest.com/docview/219838539?accountid=166551

[23]. Cohen, M. (2017). *The Human Element of Information Security | Consulting Services | Clareity*. [online] Clareity.com. Available at: https://clareity.com/security/the-human-element-of-information-security/ [Accessed 26 Jul. 2017].

[24]. Panacea Makele and Srinath Doss , "Adoption of mMoney and mHealth in a developing country: An assessment of the network and Security challenges in Botswana", *IOSR Journal of Business and Management*, Vol.19, No.19, October,2017.

[25]. Creswell, J. (2014). *Research design*. 4th ed. Thousand Oaks, California: SAGE Publications, pp.3-23.

[26]. Dawson, C. (2002). *Practical Research Methods: A user-friendly guide to mastering research techniques and projects*. Oxford: How To Books, p.97.

[27]. Drevin, L., Kruger, H. and Steyn, T. (2006). Value-focused assessment of ICT security awareness in an academic environment. *Computers & security*, (26), pp.36-43.

[28]. Edwards, K. (2015). *Examining the Security Awareness, Information Privacy, and the Security Behaviors of Home Computer Users*. Ph.D. Nova Southeastern University.

[29]. Eugene Kaspersky, Steven Furnell, (2014) "A security education Q&A", Information Management & Computer Security, Vol. 22 Issue: 2, pp.130-133, https://doi.org/10.1108/IMCS-01-2014-0006

[30]. Eyong B. Kim, (2014) "Recommendations for information security awareness training for college students",*Information Management & Computer Security*, Vol. 22 Issue: 1, pp.115-126, https://doi.org/10.1108/IMCS-01-2013-0005.

[31]. Baboloki Janet and Srinath Doss, "A Study on Cyber and Network Forensic in Computer Security Management", International Journal of Innovative Research in Applied Sciences and Engineering (IJIRASE), Vol. 1, Issue 2, August 2017.

[32]. Alfred Moselekatsi and Srinath Doss, "Comparative Analysis of Ethical Hacking over Penetration Testing, International Journal of Engineering Computational Research and Technology, Vol.2., No.2,2017.