Global Scientific JOURNALS

GSJ: Volume 10, Issue 2, February 2022, Online: ISSN 2320-9186
www.globalscientificjournal.com

A PRACTICAL MODEL FOR PROMOTING POSITIVE INFORMATION SECURITY BEHAVIOR IN LIBERIA

Nickey Yrah[1], Dr. Papias Niyigena[2]
University of Lay Adventists of Kigali

ABSTRACT

Information security for institutions is very meaningful to assure client and organizations themselves secured; with advanced technology that drives to data vulnerability issues in these organizations' data as well as the storage are most exposed to the public. Various researches including those reviewed in this study have tried to bring up solutions to the issue using different methods of authentication, but have not completely solve the problem.

Even though users might be aware of information security policies, they might not comply in various situations. For achieving the goals of this study, it was necessary to collect data from end users via questionnaires using google form and then be used to form a dataset; data analyses were carried out with use of Rapid Miner tool for dataset exploration and visualization to study the current information security situation in Liberia.

Sixty-four participants from six companies were participating in the current study, and their answers confirm to have a poor system to onboard the employees in Liberians' companies where they need a practical model to assure the data security awareness behavior among employees. Following the model proposed in this study, we assure the promotion of positive security behavior among companies' employees in Liberians.

Keyword*: Information security, User authentication, ICT policy, Liberia, RapidMiner*

INTRODUCTION

Information security is defined mainly as a set of practices intended to keep data secure from unauthorized access or alterations, both when it's being stored and when it is being transmitted from one machine or physical location to another (Fruhlinger, 2020). Information systems (IS) that interconnect emerging technologies have rendered organizations increasingly vulnerable to emerging information technology (IT) attacks (Roberto, J. M., 2014). Even if the definition is clear and various policies are set, the information security is still an issue in different ways and this needs more researchers to be involved to come up with adequate solutions such as practical model for ensuring information security in day-to-day use of ICT.

Preserving the CIA, confidentiality, integrity and availability, of an organization's sensitive information systems assets against attacks and threats is a challenge in this digital age. Nonetheless, organizations in many cases fail to protect their information assets as they rely mainly on technical solutions which are not contextually compatible and sufficient (Khando, K. et al, 2021). The lack of awareness among users in regard to security policies and best practices have been identified by security scholars as a major cause of failure. Ironically, even though users might be aware of information security policies, they might not comply in various situations; therefore, an important facet in building successful security programs involves understanding the behaviors of users that lead to compliance with security policies (Sherly, 2011).

The assessment of human behavior is a complicated phenomenon, and several psychological theories have been proposed to cover different aspects of human behavior. In this regard, multiple IS researchers proposed various research models and theories to assess individuals' behaviors towards information security policies (Rao, F. A. et al, 2021). The exponential growth in modern technologies has revolutionized our lives, particularly the communication channels used to widely disseminate information and to interact with others in real time; in response, the number of hackers and organized cybercrime groups has grown exponentially (Talal, A. and Asifa, T., 2021).

With an increasing consumer awareness on security breaches and data risks, companies must now be more proactive in how they manage their systems. The studies show that cyber-attacks are increasing in both frequency and scale. Research by digital services company Gemalto found the number of data breaches worldwide increased by 164% between 2016 and 2017. And many growing companies across the country are still not prepared to face the new and emerging

threats (Cyberriskaware, 2021). It is therefore vital that organizations have a security awareness program in place to ensure employees are aware of the importance of protecting sensitive information, what they should do to handle information securely, and the risks of mishandling information. Employees' understanding of the organizational and personal consequences of mishandling sensitive information is crucial to an organization's success (PCI-DSS, 2014).

The current study, intends to investigate how user's security behavior contributes to cyber security breaches in businesses, then examine how businesses structure their ICT policy and formulate a practical model which aligns with existing ICT policy for promoting positive security behavior. Thereby, significantly reduce the internal security threat and the level of security incidents experienced in businesses.

LITERATURE REVIEW

The previously conducted researches, we review their works especially those in the field of information security, we try to find the gaps in those works then complete and/or improve them. Below are the reviewed works.

The Role of User Behaviour in Improving Cyber Security Management, a research paper by (Ahmed, A. M. et al, 2021); researchers say that: The goal of this paper is to show that, in addition to computer science studies, behavioral sciences focused on user behaviour can provide key techniques to help increase cyber security and mitigate the impact of attackers' social engineering and cognitive hacking methods (i.e., spreading false information). Accordingly, they identify research on psychological traits and individual differences among computer system users that explain vulnerabilities to cyber security attacks and crimes. The review made shows that computer system users possess different cognitive capabilities which determine their ability to counter information security threats and they end by identifying gaps in the existing research and provide possible psychological methods to help computer system users comply with security policies and thus increase network and information security.

Methodological approach to security awareness program, research by (Predrag, 2013), the aim of the paper, therefore, is to develop innovative solutions to deliver an interactive cybersecurity awareness program, where the main goal is to enhance information on security awareness and knowledge in organizations, schools, nations, homes etc. The syllabus that is presented consists of a unique systematic approach divided into three target groups: basic, advance and management. Also, they present a different method in measuring the knowledge of each participant, and compare it to the base-line

survey carried out during the registration. By implementing this program in private and public organizations, governments, schools and universities will lead to the improvement of Information security awareness levels in the everyday use of computers, mobile phones, online banking, and social networking both at home and in the workplace.

Cyber security in the workplace: Understanding and promoting behaviour change (John, 2013); the researcher aimed at exploring employee security behaviours and then design interventions that can motivate behaviour change. They argue that previous researchers have focused on exploring factors that influence information security policy compliance; however, there are several limitations with the approach. That why their work-to-date has explored the behaviours that constitute 'information security' and potential influencers of these behaviours. These findings will aid the design of behavior change interventions.

Within the current research, we will demonstrate the power of thinking about systems users, end and administrative, behavior towards information security mechanisms with purpose of developing a practical model to promote the positive behavior in users to keep their authentication means safe and keep them in Integrity, Confidentiality, and Available only for the owner, and this will be mixed to make a single security mechanism to enhance the protection of data by allowing the access of authorized user on organizations resources.

METHODOLOGIES

This section clarifies the way projected results will be achieved; this involves to outline tools to be used while carrying out this research.

Research design

We proposed empirical based research, where it needs data to be studied and visualized to obtain trends such that will stimulate the development of practical model for promoting the information security behavior among end users. Some evidences to be included in this research are collected from users' perceptions via questionnaires to form numerical dataset, which means the research approach to be followed is quantitative approach, such that it will deal with numerical variables.

Research Conceptual framework

This study consists of data collection from end users of ICT tools, after being collected data will be prepared, and then visualized to get insights, and finally a practical model for promoting the information security behavior among users will be designed; the procedure is presented as following in phases below:

Phase 1 - Data collection; for understanding the current issues, it is necessary to collect data to be used in dataset building and this will be from end users via questionnaires to be shared with google form.

Phase 2 – Data treatment; after data are collected the next step was data treatment by arranging them in concrete manner, removing the unnecessary data, missing data, especially focusing on the data which fulfill the qualities aligned to the research objectives.

Phase 3 – Data visualization; Data analysts use various tools to understand data in means they expose trends inside data; in this study I suggest to use RapidMiner tool for dataset exploration and visualization. In this phase, dataset variables were plotted in 3D graphs such that trends and insights from dataset will be observed and visualized to study the current information security situation.

In addition to this, secondary data will be considered to go through policies and programs to emphasize the information security in Liberia, here it will be read and come out with the situation on how the government and different organizations are prepared to keep their data secured against any breach.

Phase 4 – Practical model for promoting the information security design; From previous phases, after visualizing the data and understand the situation for information security and ICT policies in Liberia; now the last step is to focus on design of a Practical model that is expected to enhance a positive behavior of users towards data security.

RESULTS AND DISCUSSION

Demographic information

The Graph here below presents the gender distribution of participants within this study;

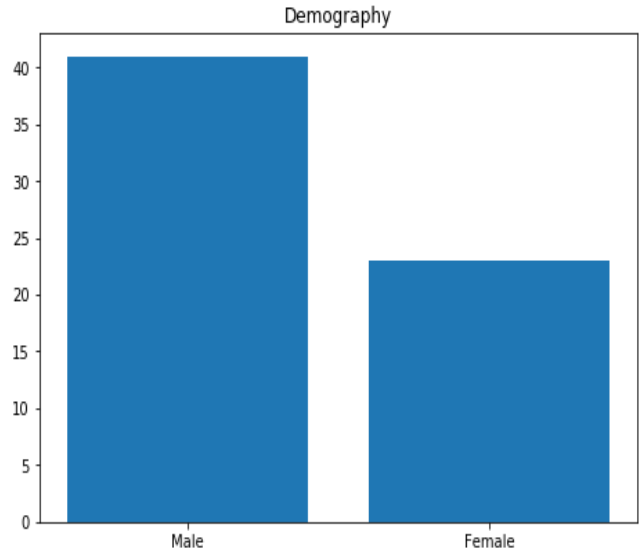


Figure 1 - Demographic information

Referencing to the graph above, the total number of participants for the study was sixty-four (64); 41 male and 23 female workers from 6 companies.

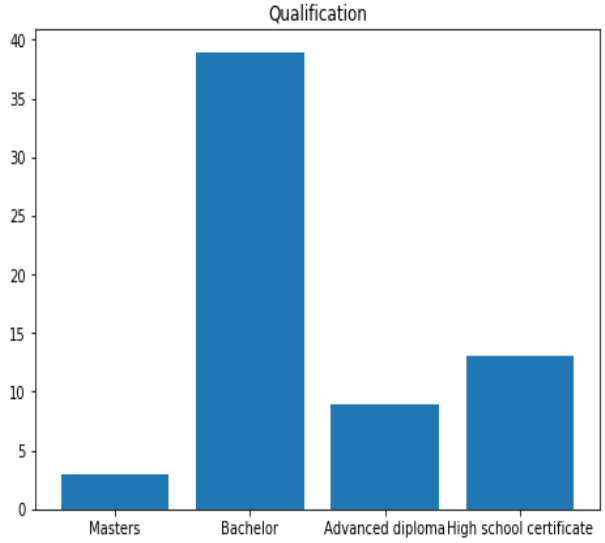


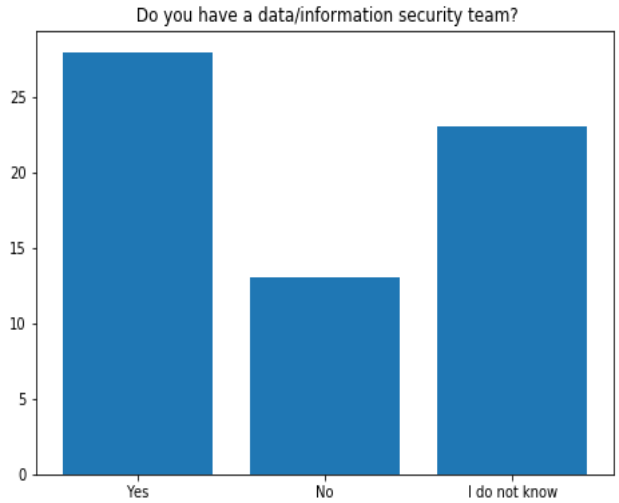
Figure 2 – Participants' qualification

For participants educational background, the majority of them had Bachelor's degree with 61%, those with a high school certificate is 20%; the least category was those with Master's degree with a representation of only 5%. None of the participants had a doctorate degree. This demographic information is describing a good team for a productive company and assure the accurate data from the survey as well as respondents are aware of what they are asked.

End users' awareness on information security issues

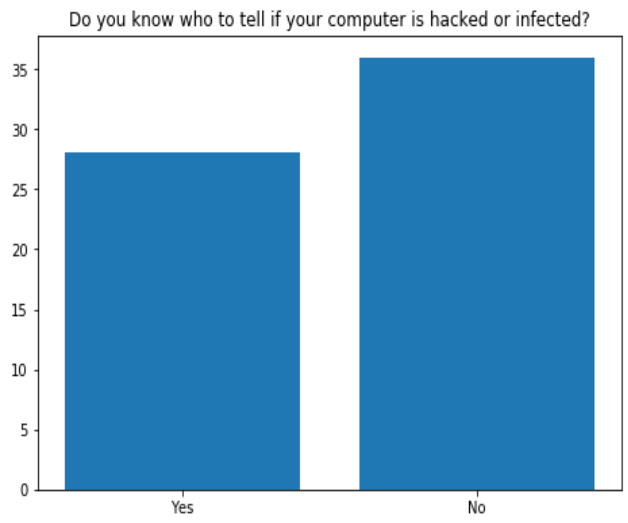
As introduced above, a google form has been shared among six companies' workers to understand their awareness on information security in their daily activities. Below are the responses from 64 respondents participated in this survey.

Q1. Do you have a data/information security team?



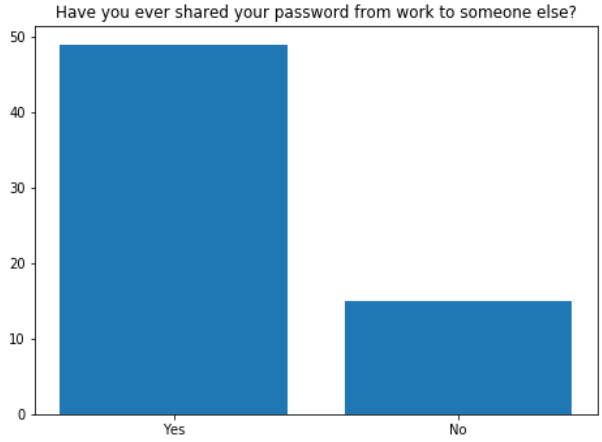
The graph above indicates the responses ratio from the questionnaire used in the current study; 44% of the respondents admitted that they know the presence of the information security awareness team; 20% responded to not have any team in their company, while 36% of the respondents are not aware of the information required. From the results, 20% and 36% which makes 56% of the total participants, who doesn't have any information on the presence of the security team this is significant to the companies that their employees are not aware on whom to contact when they encounter any information security issues.

Q2. Do you know who to tell if your computer is hacked or infected?



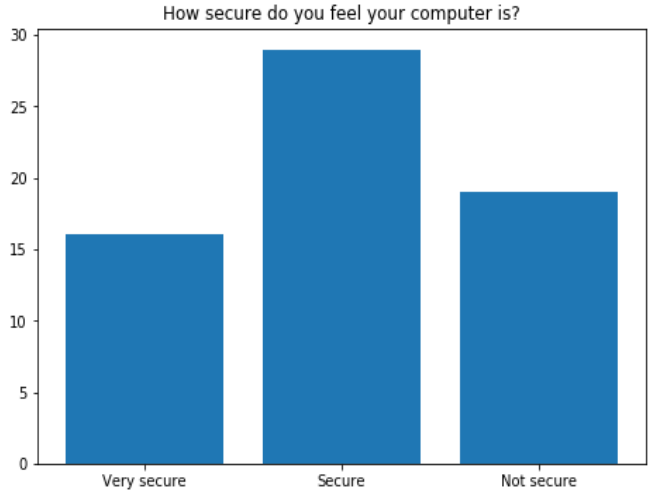
From the responses on the second question, they didn't go far from the findings of the first question where it is indicated that only 44% of participants know to whom to contact when they are hacked or simply hacked or infected by intruders.

Q3. Have you ever shared your password from work to someone else?



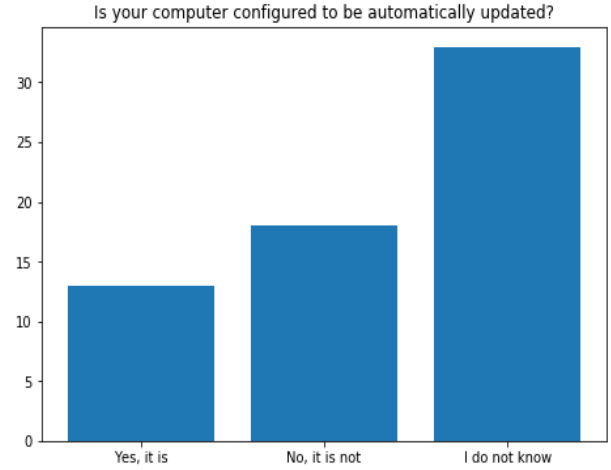
The findings on the third question, indicate that 49 over 64 participants which made of 77% of participants, at least once, they shared their password with other workmates; which indicate that within companies themselves employees may become insider threats and hack themselves.

Q4. How secure do you feel your computer is?



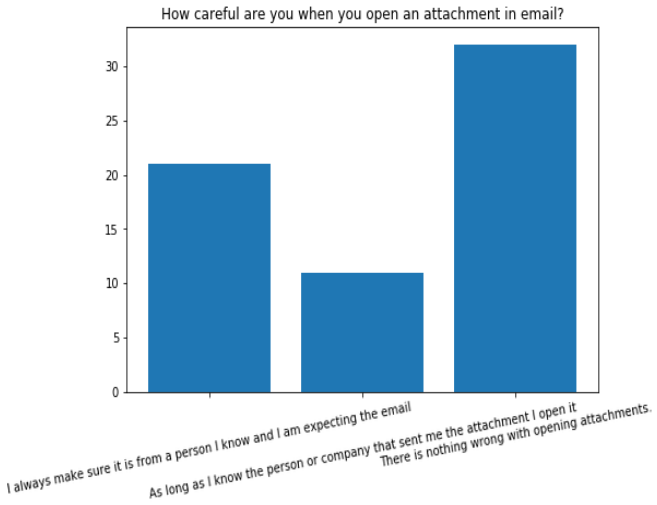
The fourth question was about to know on which scale employees are secured with their data and computers; the findings shown that 25% of participants are very secured, 45% they feel to be secure, and 30% of respondents are feeling to be not secured.

Q5. Is your computer configured to be automatically updated?



The above results presentation of the findings from the participants in the current study, from which 13 respondents confirmed that their computer are configured to be automatically updated, 18 respondents say that their computers are not updated, while the remaining 33 respondents that make 52% said that they are not sure if they are computers are whether updated or not. This shown that awareness on computer basic skills and information security issues is on the low scale, and the companies are obliged to train their staffs on how to use computers and keep them healthy.

Q6. How careful are you when you open an attachment in email?

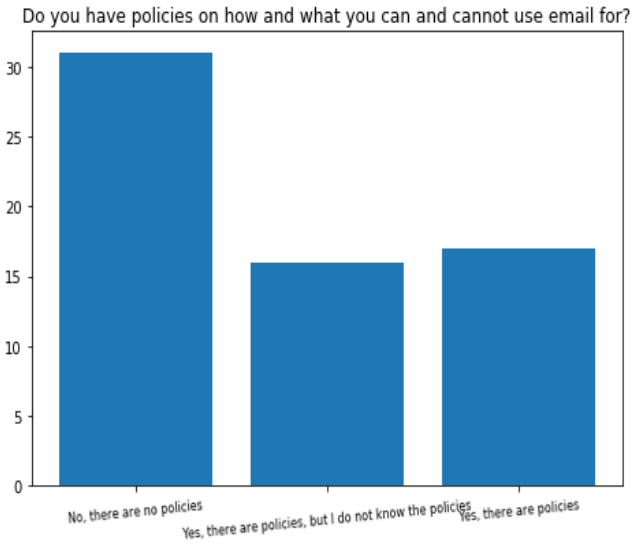


About how the employees of the selected companies are careful on emails and their attachments, the findings indicate that 50% of the participants are not caring on opening the attachment, and only 33% only are careful to open the attachments by always making sure of its source and expecting the email. This may lead the companies to be infected easily as well as a half of their employees are not caring on the attachments and other emails they receive and open them without any concern on the sender.

Q7. Do you have policies on which websites you can visit in your company?

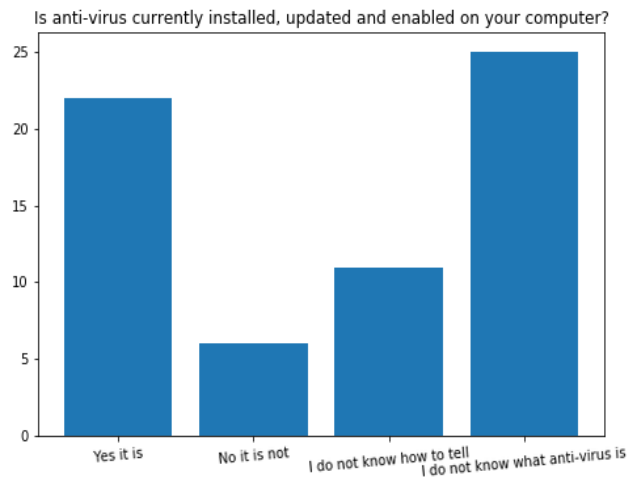
For the websites restrictions policies, mainly the respondents up to 56% confirm that there are no policies, 14% affirm that there are policies but they are not aware of the policies contents; while 30% they are aware of the policies and their presence at their companies. This indicates the lack of trainings or onboarding staffs on the company's operations and policies on the use of internet at the workplace.

Q8. Do we have policies on how and what you can and cannot use email for?



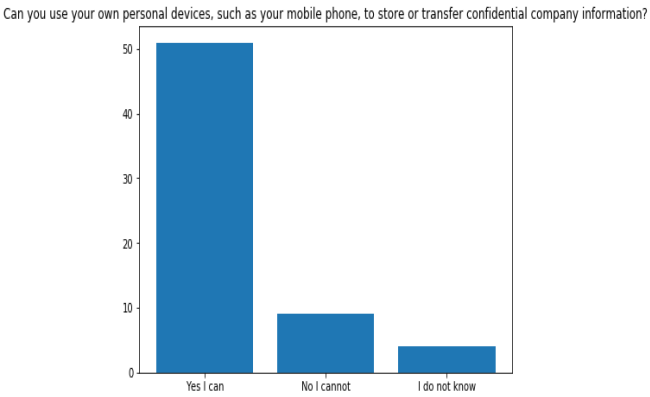
The above results are findings from the respondents on emails use policies, up to 48% of the respondents confirm that there are no policies, and they can send whatever emails I want to whomever I want while at work, 25% affirm that there are policies but they are not aware of the policies contents; while 27% say that there are policies and I know and understand them. As long as the ratio of employees that don't understand and not aware of the policies is high, it indicates the lack of trainings or onboarding staffs on the company's operations and policies on how and what you can and cannot use email for while they at the workplace.

Q9. Is anti-virus currently installed, updated and enabled on your computer?



Respondents on the use of anti-viruses in their computers, the question was about to know if anti-viruses are installed, updated, and enabled; the findings indicate that 34% of the respondents are aware of their computers' status, 9% confirm to not have anti-viruses installed, 17% they are not sure to have it installed, 39% of the respondents have no idea on what anti-virus. Means, companies need to onboard their staffs on how to use anti-viruses, update, and enable them to keep their computers safe.

Q10. Can you use your own personal devices, such as your mobile phone, to store or transfer confidential company information?



With the last question, the employees who participated in the current research, 80% affirm that they can you use your own personal devices, such as your mobile phone, to store or transfer confidential company information, 14% denied this act, and 4 that make 6% of the respondents say that they are not aware if they did or not.

Practical model for promoting positive information security behavior in Liberia

From the above research findings, it is mainly shown that employees are not familiar with the use of computers and other digital devices that are capable of sharing information among different company staffs. As remedial to the mentioned problems with the above findings, this research is proposing a practical model on how to enhance the ability of users/employees in Liberia on promoting users' awareness and towards data security.

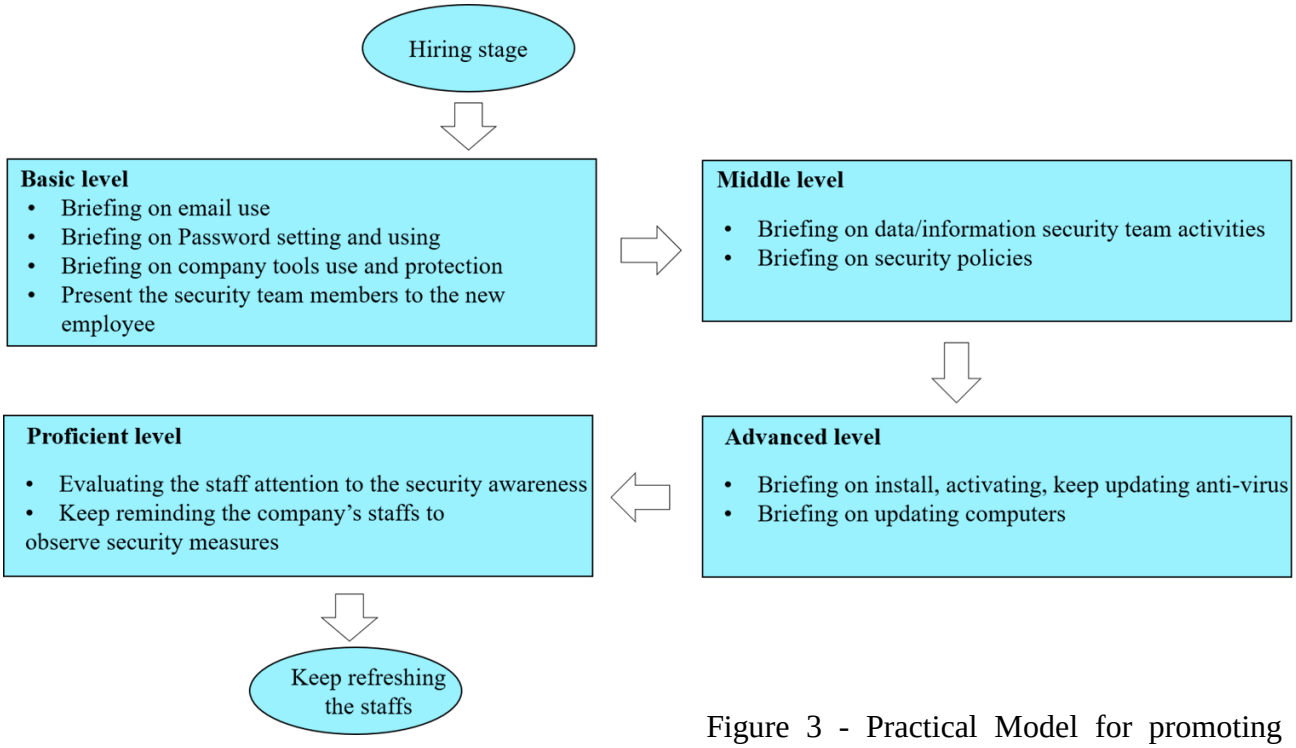


Figure 3 - Practical Model for promoting positive information security behavior.

The proposed Practical model for promoting employee information security awareness includes four main parts, it starts with the employee hiring stage and ends with keep refreshing the staffs; under different levels of employee onboarding, the company will need to create a series of trainings to build the capacity of its employees and promote information security awareness behaviour in their daily activities. Following the model proposed above, we assure the promotion of this behavior among companies' employees even within all Liberians end users of various digital devices those can be used to share information.

Hiring Stage

This is the beginning of the employee onboarding and this is where a good information security behavior starts. Therefore, the briefing on basic policies and best practices begins at this stage. The employee must have a briefing session with the Information security Team to be informed about the dos and don'ts in the working environment.

Basic Level

After the onboarding process during the hiring stage, the employee will now have series of sessions at this stage. The employee will be presented to the Security Team and get to know their names and role play in the team.

After this process, the team will proceed with briefing of email usage, password setting and usage and company tools (devices given to you as per your role in the company) use and protection.

Middle Level

At this stage, employee(s) will go through briefing on data/information security team activities. The will be given time line and the type of activity that will be perform by the team.

They will also be briefed on the company's security policies and how to adhere to them and the penalties attached to breaching said policy.

Advance Level

After employee(s) has been acquainted with the company's security team and the policies that exist, they will now proceed to an advance level of their onboarding process.

At this stage, the employee will be trained on how to install, activate and update antivirus as per the guideline in the security policy.

They will also be trained on how to update the computer system there are using.

Proficient Level

This is a very important part of the model and need serious attention.

At this level, the security team will evaluate the staff attention to the security awareness, briefing and the trainings that was done from the beginning of the process.

The team will also keep reminding company's staff to observe security measures.

Keep Refreshing the Staffs

To achieve this model perfectly well this stage must be taken into consideration. The process in this model should be implemented as per the guideline of the company's security policy. By refreshing the staffs through various stages of this model, a company would maintain a positive information security behavior.

CONCLUSION

The data is exposed to different authorized and unauthorized access, the purpose of this research is to investigate how user's security behavior contributes to cyber security breaches in businesses and then examine how businesses structure their ICT policy and then formulate a practical model for promoting positive security behavior.

Traditional methods of user authentication, such as passwords, PINs, and tokens, sophisticated technologies such as fingerprinting to identify customers are also used are now obsolete, easy to forge, and cannot protect consumer information. For the information security purposes the current study proposed the practical model to promote the positive behavior in users to keep their authentication means safe and keep them in Integrity, Confidentiality, and Available; where through four stages starting with the employee hiring stage and ends with keep refreshing the staffs; under different levels of employee onboarding, the company will need to create a series of trainings to build the capacity of its employees and promote information security awareness behaviour in their daily activities.

REFERENCES

Ahmed, A. M. et al. (2021). The Role of User Behaviour in Improving Cyber Security Management. *Frontiers in Phychology*, 11 - 25.

Cyberriskaware. (2021). *THE ULTIMATE GUIDE TO SECURITY AWARENESS TRAINING.* NewYork: Cyber Risk Aware.

Fruhlinger, J. (2020, Jnayary 17). *What is information security? Definition, principles, and jobs*. Retrieved from CS ONLINE: https://www.csoonline.com/article/3513899/what-is-information-security-definition-principles-and-jobs.html

John, M. B. (2013). Cyber security in the workplace: Understanding and promoting behaviour change. *PaCT Lab*, 25-36.

Khando, K. et al. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Elsevier, Computers and Security*, 1-7.

PCI-DSS. (2014). *PCI Data Security Standard (PCI DSS).* Chicago, USA: Security Awareness Program Special Interest Group.

Predrag, T. (2013). Methodological approach to security awareness program. *Security in Computer Systems and Communications*, 1-8.

Rao, F. A. et al. (2021). Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance. *MDPI - Applied science*, 13-29.

Roberto, J. M. (2014). A Model of Information Security Awareness for Assessing Information Security Risk for Emerging Technologies. *Journal of Information Privacy and Security*, 160 - 185.

Sherly, A. (2011). INFORMATION SECURITY BEHAVIOR: FACTORS AND RESEARCH DIRECTIONS. *Proceedings of the Seventeenth Americas Conference on Information Systems* (pp. 1-13). Detroit, Michigan: AIS Electronic Library (AISeL).

Talal, A. and Asifa, T. (2021). Assessment of Cybersecurity Awareness among Students of Majmaah University. *MDPI - bdcc*, 1-15.