Improving Social Engineering Awareness, Training and Education (SEATE) using a Behavioral Change Model

Azaabi Cletus, Benjamin Weyory, PhD, Alex Opoku, PhD
School of Sciences, University of Energy and Natural Resources, Sunyani, Ghana

***Abstract*—Social Engineering (SE) Awareness, Training, and Education (SEATE) is one of the recommended defenses against SE attacks among users of Information Systems. However, many of these SEATE programs fails to achieve the desired impact leading to exposures. This study sought to explore SEATE programs to identify gaps/challenges and propose relevant content, Delivery Methods, and a novel behavioral change Model to improve SEATE programs among users. An explorative Literature Search was conducted on the relevant SEATE Content, Delivery methods and the challenges of SEATE Programs. Consequently, the relevant and critical content and delivery methods were proposed. The challenges that impede the efficient and effective conduct of SEATE Programs were established. A behavioral change Model known as Social Engineering Awareness, Transition, Adaptation and Consolidation (ATAC) based on Stable-Quasi-Stationary Equilibrium theory was proposed. The model was validated using Expert Opinions. Five (5) expert in cybersecurity were recruited to appraise the model based on five metrics; fit for purpose, novelty, ease of use and structure. The results show that, challenges still exist in the conduct of SEATE programs. To improve SEATE programs requires relevant and innovative content, and delivery method (Hybrid Approach). Validation of the proposed behavioral change model showed an average score at 73.6% and performance metrics at 92%. As the menace of SE attacks rages on and exploiting the user, the need for SEATE programs remains imperative. A well-developed and relevant content, delivery methods and a clear understanding of the challenges is required to improve SEATE. Following the model developed, and the repeated use of it will lead to improving user resistance and or immunity to SE attacks and by extension improve security culture among users.**

Keywords*—*Social engineering; user training; user awareness; user education; ATAC model

I. INTRODUCTION

Globally, cyber-attacks remains a major threat affecting individuals, small and medium enterprises, multi-national corporations, nation states and indeed all global stakeholders in the cyber space [1], [2], [3], [4], [5]. This is occasioned by the ushering in of the 4th Revolution (information superhighway), the growth and expansion of the internet, the Internet of Things (IOT), cloud computing and extensive penetration of smart phone telephony [6].

Even though these statistics are positive signals towards cyber inclusion, the problem of ensuring that, the data and information stored in computers and in Critical Information Infrastructure(CII) are protected against unauthorized access, modification, vandalism and others poses a big challenge particularly attacks against the human wall (the weakest link) also known as social engineering (SE). [7] describe, SE as gaining access to systems, buildings, data by exploiting humans using psychology instead of using technical procedures to break in. [8] Sees it as influencing a person to an action that may or may not be in his/her interest. Consequently, the increased use and adoption of these technological assets has expanded the cyber-attack surface in general and SE in particular, resulting in exposures to critical information asset and the concomitant effect of reputational loss, financial loss, legal issues [9].

Consequently, cyber criminals realizing that, the 'wet ware' is easier to compromise have resorted to employing SE attack methods to perpetuate cybercrimes by gaining access to confidential information [10]. Hence, the need for programs to protect users against such SE attacks.

Over the years, defenses against social Engineering attacks have been varied. The most common SE defenses has been user education [11] [12], user Awareness [9] [5], user Training [13]. Other recent defense programs included Gamification [14]), the use of Apps [15], Serious games [16], Virtual labs [17], conferences and tournaments [5]. The rest of the programs include the use of predictive and preventive tools [18] and Recognition tools [19].

As organization realizes the impact of user awareness as a means to complement the technology-based defenses, many have increased budgetary allocation, time and effort to ensure security among users using policies and other behaviour-based approaches such as awareness, training and education [20], [21].

Even though these programs are aimed at building the resistance of users and ensuring that they are well prepared to defend against various SE attacks, they fail to achieve their intended purpose due to how these programs are organized, the content and the pedagogy used; thus, leading to exposures of confidential information and its consequential impact.

This paper sought to explore SEATE programs establishing the challenges, exploring and proposing relevant Content, delivery methods, and a model to be used to conduct SEATE effectively and efficiently that will lead to permanent SE security culture, resistance to SE attacks and reflective

behavior of users when faced with an SE attack. To do this, the following research objectives were set:

- Explore and proposed relevant SE Content, Delivery methods and challenges of SEATE programs.
- To propose a behavioral change model to improve SEATE programs among users.

The contribution/value/novelty of this work;

There is a limited academic study on the use of behavioral change models in improving SEATE programs. Consequently, this study and its findings is a modest contribution to SEATE programs in particular and improvement of user resistance in general. Hence, this study is a modest contribution to knowledge in the field of SE in particular and Cybersecurity in general.

Specifically, the study contributed to knowledge in the following ways:

1) Critically analyzed literature and established relevant content, Delivery methods and challenges of SEATE. Through this approach, we proposed innovative and relevant SEATE Content and the key points that should be included and emphasized during SEATE Programs.

2) We also highlighted the industry delivery methods and their challenges and thus proposed a hybrid approach so as to complement the deficiencies in each of them.

3) Proposed a model to be followed to improve SEATE resulting in improvement of 92% in model performance metrics rating.

4) Contributed in design process, methodology that can be used by practitioners to improve upon their SEATE projects.

The rest of the paper is structured as follows:

In Section 2, Theoretical and Related Works; Section 3, Content, Delivery Methods and challenges of SEATE Programs; Section 4, Proposed Model and Validation, Section five 5, Results, section 6, Discussions of the Findings, Section 7, Conclusion and Future Works and at the end are the references of the study.

II. Theoretical Framework and Related Work

A. Theoretical Framework

The concept of SE mainly refers to attacks aimed at tricking the user (Holder of a vital information Asset) to divulge such information against the wish of the user [8]. As an attack against the user, any defense or protective mechanism should aim at the user. This will ensure that, the user is aware of such attacks, modify their behavior about SE attacks and manage the needed change to prevent, and or mitigate the attack.

The study [22] is regarded as the father of change management (CM). He proposed the 3 –step model indicating that, a successful change passes through 3 steps; unfreezing, moving and refreezing [22]. He contended that to manage change process, the organization must unfreeze; change from current state to a neutral position, to enable the unlearning of the old behavior, and to ensure that the new behavior can be adopted and adapted successfully. Once the change occurs, the organization refreezes into the new state. This is often referred to as Stable –Quasi- stationary- Equilibrium.

Extending and applying this theory, we indicated, that, SE as a cyber-phenomenon, requires that all stakeholders are offered the required SEATE with the aim of improving resistance to such attacks, creating permanent cyber/SE security culture and consciousness and permanent behavior change against SE attacks.

Reasoning on this principle, we proposed a model known as Awareness, Transition, Adaptation and Consolidation (ATAC) model to improve SEATE programs. A review of related works in social engineering awareness, trainings programs follows in the next section.

B. Related Work

Research into security Awareness program in general and social engineering in particular has gained pace in recent years especially in programs aimed at improving security against SE attacks [5], [9], [21],[6].

The author in [6], proposed an educational model for systematic adaptation to cyber security training programs. However, this model is for generic cyber security awareness and fails to address the issue of SE. Specifically, using the modus operandi in social engineering differs with other technology or traditional hacking methods.

A web-Based System (SAWIT tool kit) was proposed and translated into a prototype to improve security awareness. It was based on knowledge sharing among employees [21].

The author in [5] delivered a conference paper on challenges of implementing training and awareness programs targeting cybersecurity social engineering. They suggested budgetary constraints for trainings, lack of understanding of information security, bad organizational cyber security culture as some of the challenges facing SEATE. He recommended the use of security preparedness exercises and awareness programs as a means to improve security.

The author in [23] proposed a framework to evaluate the risk inherent in the Internet of Things (IOTs) based on the situational awareness. The focused on awareness in IOT devices and how promote situational awareness of security. Other studies considered SE awareness on the bases of the business environment such as technology, organization etc. as a way to improve SEATE. Social issues as a limitation against SEATE was also conducted [11].

Notwithstanding the number of studies conducted in social engineering awareness trainings, not much is done in clearly identifying the key critical challenges of a SEATE programs, the required and relevant content and delivery methods and a model that can improve user behavior change to ensure permanent cybersecurity culture in general and SE in particular. Thus this paper explored relevant SEATE programs, content, delivery methods and the challenges and proposed a novel behavioral change model for the improvement of SEATE programs. The next section explored

the Content, Delivery methodologies and challenges/setbacks of SEATE programs.

III. Content, Delivery Methods and Challenges of SEATE Programs

A. Cybersecurity Social Engineering Content

Social Engineering attackers continue to plaque the cyber world with new and novel attacks. Even though organization is spending huge sums of money to ensure security, their effort always most times fails due to user vulnerability to social engineering attacks. To ensure improved security, organizations' employees' knowledge need to be improved using awareness, training and education programs [20]. This should include exposure to security policies, processes and best standards that promote corporate cybersecurity in general and social engineering in particular. The content should contain awareness programs at the base for starters. These are programs aimed at exposing the user to SE attacks towards changing the behaviour of the user [2].

Training programs should follow this, which enables the user to make appropriate security choices in their daily personal and work life. Users are trained on specific actions to take in specific cases and should be selected and implemented based on the set objectives.

Finally, the SEATE program should graduate to education where individuals interested to take careers in cybersecurity are given specialized education in specific area by providing in-depth knowledge in the area of security. Thus, SEATE programs should follow a learning continuum, which begins with awareness creation, cumulatively building into training and eventually evolves into education as shown in Fig. 1 known as the cybersecurity learning continuum.

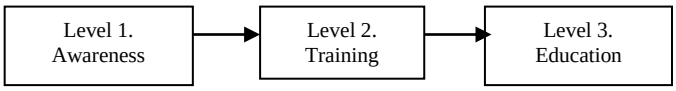

Fig. 1. Learning Continuum.

The author in [20] suggests that most information security awareness programs are generic in nature, too much information leading to information overload. This makes it difficult for users to decipher the relevant content to concentrate. Even with the relevant content, the delivery approach is also relevant to ensure that the right and relevant content is well delivery to the user.

B. SEATE Program Delivery Methods

There are many and varied methods used in the delivery of SEATE programs. [2] Suggested face-face method (lectures, storytelling and workshops), self-directed learning which can be static in nature (text and web based) or flexible/dynamic (videos and games) and finally, teachable options such as embedded delivery methods such as online learning. In the face-face, approach involves a physical environment with or without an expert who facilitates the process. The self-directed learning involves a virtual platform where the SEATE program is delivered such as web-based trainings, text-based and video based approaches. In the case of teachable delivery method, embedded links and content is attacked for user to learn.

[24] contend that, security awareness delivery methods include the conventional methods such as posters, stickers, leaflets, newsletters; Instructor- led; formal presentations, training sessions and online delivery methods such as electronic articles or emails, web-based security awareness methods, alert messages and game-based methods.

It is worthy of note that even though many of these approaches are proposed towards achieving maximum benefit from such programs, many fail due to inherent challenges such as too much information, cost, boring, inexperience instructors, monotony leading to security breaches.

C. Challenges to Cybersecurity SEATE Programs

The use of SE security training awareness, education and other programs aimed at protecting users against SE attacks is well documented in literature [25],[9]. These programs aim at improving user resistance, and increased SE attack consciousness. [5]opine that, several factors militate against SE training and awareness; the Business Environment, Social issues including industry competition, the compliance or legal frameworks with the country, organizational issues, economic and personality issues or traits that serves as challenges to a successful SE education, training and awareness.

Other methods to SE education, training and awareness include the current methods such as games, Apps, Virtual labs, tournaments, conferences [5]. However, these have challenges such as coordination in the case of serious games, and personality issues about collaborative approaches. Others include real-life simulations and videos. These simulations are generic and fail to cater for the individuals in the organization.

The earlier methods to SEATE programs include manual reminders, the use of posters, awareness campaigns, online courses and physical access programs [20]. However, these methods are said to be boring, tedious and time consuming and lack practical exposure for employees.

From the forgoing, time constraints, Budgetary constraints, generalized nature of the training and awareness program without recourse to the individual users, characteristics such as educational level, organization level (operational, management and levels) pose a major challenge in the successful conduct of SEATE projects. Thus, to be able to effectively and efficiently carry out SEATE programs to achieve the intended objective, there is the need for relevant content, innovative delivery methods and organizational and behavioral change models [21]. The next section will consider the characteristics of relevant content, innovative delivery method and propose a social engineering security behavior change model for effective and efficient SEATE programs.

IV. Methodology

The study aimed at exploring the SEATE content, delivery methods and the challenges faced in achieving the intended objectives and to propose innovative content and delivery methods and a novel behavioral change model to improve SEATE programs.

TABLE I. PROPOSED RELEVANT SEATE CONTENT AREA AND DESCRIPTION

Comprehensive Knowledge of a Social Engineer.	Clear understanding of the goals, objectives and motives of a Social Engineer, types, characteristics and tricks
Comprehensive knowledge of vectors in use.	Understanding of both semantic, syntactic and AI based vectors, forms of vectors, categories, their deployment strategies and how to overcome them.
Comprehensive knowledge of users/ victims.	Understanding of user vulnerabilities, traits that makes users vulnerable, level of training and exposure to cybersecurity issues etc.
PsychoSocial factors used in social engineering attacks.	Clear understanding of the psychosocial factors used in carrying out an attack; strong effect, diffusion or responsibility, overloading authority, urgency etc.
Relevant standards and regulations.	ISO/IEC27001 &27002, PCI/DSS, FISMA, GRAMM-LEACH BLILEY ACT, HIPAA, Red Flag Rule, GDPR. These will provide users and third party contractors with policies, procedures, cardholders information, information assets risk management, responsibilities and compliance, employee management and training, system failures, create awareness to raise red flag as when a threat shows up, general data protection to monitor, compliance, awareness, training and audit to ensure data security.

To achieve this, literature was explored to establish the challenges of SEATE programs. Then a meta-data analysis of the industry-based SEATE Contents was explored and compared with our proposed innovative content as illustrated in Table I.

Secondly, we compared the traditional delivery methods, identified their gaps, and proposed an innovative Hybrid method for delivering SEATE programs. The proposed hybrid approach is shown in Fig. 2. The use of the hybrid was proposed because the weaknesses in the traditional methods will be complemented by combining them.

To improve overall SEATE programs objectives, we proposed a behavioral change model known as Awareness, Transition, Adaptation and Consolidation (ATAC) to improve SEATE programs. The figure below shows the model and brief description of it.

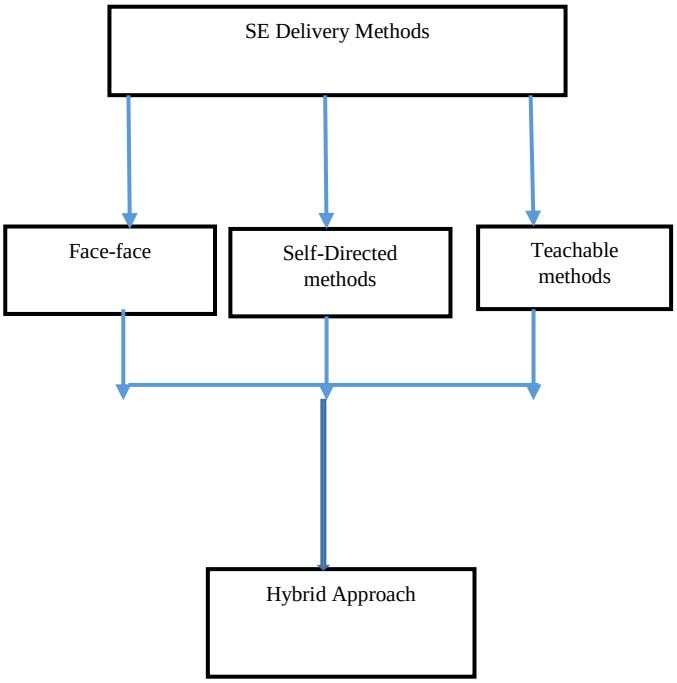

Fig. 2. Proposed Hybrid Delivery Approach.

A. Proposed Model and Description

We proposed a model known as "Awareness, Transition, Adaptation and Consolidation (ATAC) as a solution to improving SEATE and by extension S.E Attacks. The Model is as shown in Fig. 3.

The model is in four (4) phases; Awareness, Transition, Adaptation and Consolidation with an arrow depicting the needed force of change such as cybersecurity consciousness (internal or external). This is how the model works:

1) Awareness phase: Making users aware of their behavior deficiency to SE risks is needed. When users' awareness of the implication of their current deficient state is made known and the associated Danger, they begin to think of how to change.

2) Transition state: Users are now aware of the dangers associated with their behavior; Hence, wanting to change from their current state to the proposed new state.

3) Adaptation phase: In this stage, the user has transitioned into the new or required state and are now prepared to live such a new life; being security conscious and taking calculated actions to ensure that his behaviour does not lead to exposure.

4) The consolidation phases: this phase ensure that, the use is now ready and living the desire organization security culture. Enforcing this new behaviour through monitoring, reminders, penetration testing will ensure that the user do not relapse to the old state.

Such a cycle of creating awareness among users and exposing them to the dangers leads them to want to change. This leads to transition where the user switches from the lack of knowledge to the new state. This desire enables the user to adapt to the new way of cybersecurity conscious life. Consistent use of this will lead to consolidation, where the desired behavior is enforced to become part of the user and the process continues back to the awareness when new requirement for change is necessitated. To ensure the potential usefulness and usability of the proposed model, it needs to be validated.

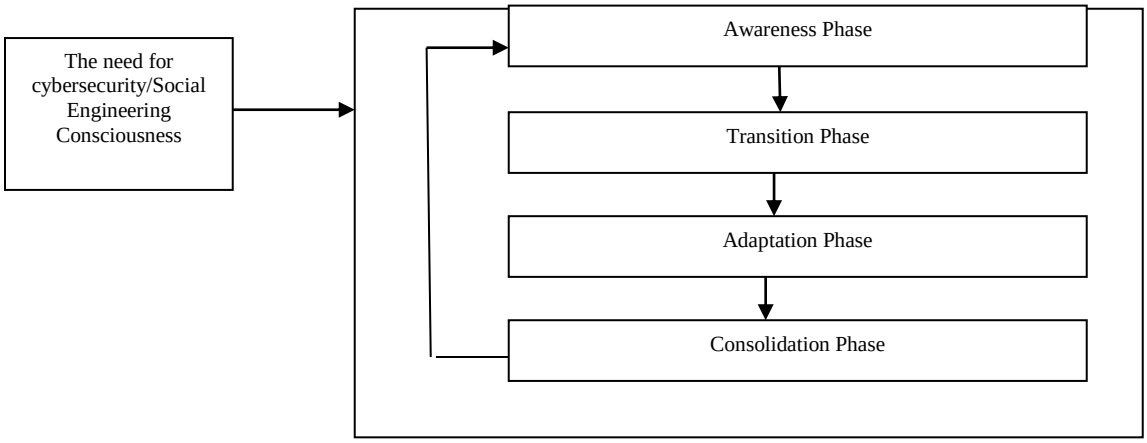

Fig. 3. Proposed ATAC Model.

TABLE II. COMPARISON OF HYBRID DELIVERY MODEL WITH EXISTING DELIVERY METHODS

Delivery Method	Lecture	Workshop	Story	Embeddded Links	Flexible	Videos Games	Static
Face-Face	✓	✓	✓	X	X	X	X
Self-Directed Teachable Moments	X	X	X	X	✓	✓	✓
Hybrid	X	X	X	✓	X	X	X

B. Model Validation

To validate the model, Expert Opinions were elicited to ascertain the usefulness and usability of the artefact. This was done using Observational Empirical Research whereby the

The researcher did not intervene in the assessment of the model by the Experts. The aim was to gain useful information about the expected usability and usefulness of the proposed artefact in a real-world context [26]. Experts were to rate the model in dimensions/metrics such as fit for purpose, novelty, ease of use, architectural structure. Each metric was to be rated on a scale of 1to 5 based on the expert's view of the model to that metric. The result is shown in Table I. Descriptive statistics were used to represent the data. We measured the central tendency using Arithmetic means as this describes the center of the data if divided equally among the subjects (Howard & Fletcher, 2016). The results of the study are presented in the next section.

The result of the proposed relevant SEATE Program Content, the proposed Hybrid delivery method and the Expert Opinion were analyzed and presented as shown in Table I, Fig. 3 and Table II, respectively.

V. RESULT

This study sought to explore SEATE programs and to propose relevant Content, Delivery Methods, Challenges and to propose innovative SEATE Content, Hybrid Delivery method, and a novel behavioral change Model to improve SEATE programs among users. The result of the study was presented according to these objectives using tables and graphs.

In research objective 1, the aim was to propose a relevant SEATE content for the improvement of SEATE programs to obtain the desired impact and results. This is demonstrated in Table I.

The next objective was to compare the existing SEATE delivery methods with our proposed hybrid approach. The result of the proposed SEATE Delivery methods and the proposed innovative approach is as shown in Table II.

To improve the conduct of SEATE programs, we proposed a behavioral change model and evaluated it. The model was validated using Expert opinion as a means to scaling to practice. Experts were to rate the model based on the dimensions given on a scale of 1 to 5 for all the dimensions. The result of the opinions is presented in table. The overall Expert score of the model by Experts is presented in Fig. 4 whiles that of performance metric measures is shown in Fig. 5.

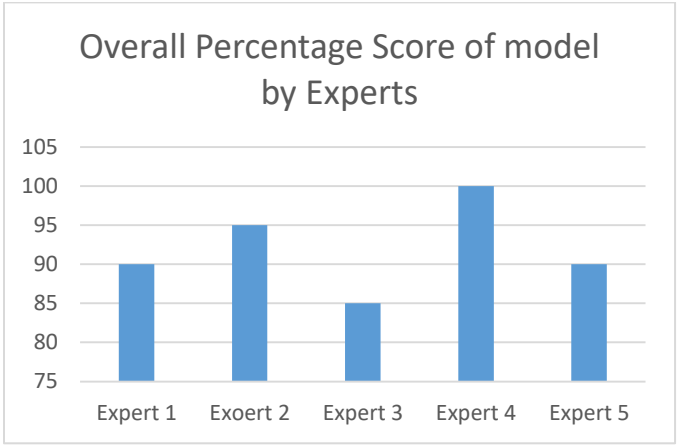

Fig. 4. Overall Percentage Sore of the Model by Experts.

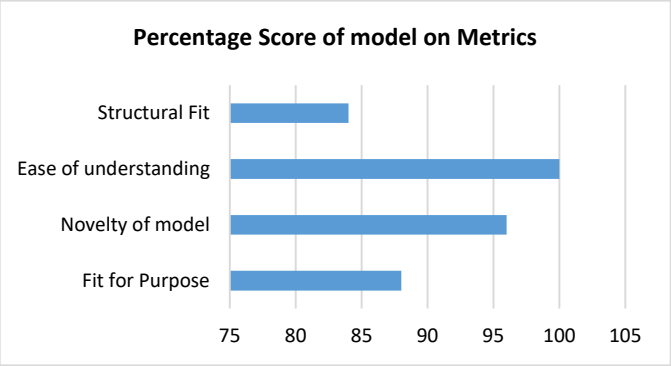

Fig. 5. Percentage Score of the Model on Metrics.

VI. Discussion

The study sought to explore the content, delivery methods, challenges of SEATE programs and suggest Relevant SE content, innovative Delivery method and a model for improving SEATE programs.

The findings from the study demonstrated that, the content of SEATE programs is relevant to the success of the program. To have an effective SEATE Content, a critical analysis of the SE attack cycle is relevant. We argue that, having knowledge of the Social Engineer such as goals/motives(financial, espionage, competitive advantage, revenge), types of social engineers(hackers, penetration testers, disgruntled employees, government's foreign intelligence people, spies) and all relevant information about Social Engineers when included in the SEATE program improves the understanding and knowledge of the user [27]. Also of relevance to improving SEATE Programs content is knowledge of social engineering vectors (syntactic, semantic and AI Based attacks). These vectors include phishing, pharming, water holing, spyware, adware, rootkits, Trojans, etc. [7]. Thirdly, knowledge and comprehensive understanding of the User and the vulnerability to SE attacks is relevant as part of the content to be included in the SEATE programs. Moreover, an effective SEATE program should also include the psychosocial factors used in SE attacks. These among others include, elucidation, strong effect, urgency, reciprocation, diffusion of responsibility, authority [8],[9]. Finally, knowledge of the relevant industry standards and regulations needs to be explained to users. These include ISO/IEC27001 & 27002 to provide all employees, contractors and third parties the policies, procedures, for their job; PCI/DSS for employees to understand the cardholder information and to acknowledge it. Federal information security management Act for employees to understand the information assets, risks, responsibilities and compliance. Gramm-Leach Bliley Act for users to understand the risks to customer information, employee management and training, information systems knowledge, and managing systems failures. Health Insurance Portability and Accountability Act (HIPAA) implement security awareness and training programs for all employees. The use of the Red Flag Rule for user to be able to identify threats and raise Red Flags when there is need and General Data Protection Regulation (GDPR) to create awareness, training, monitor compliance, and audit to ensure Data security as depicted in Table I.

The delivery methods used in conducting SEATE programs has an impact on the outcomes of such programs. Such programs are many and varied. The author in [2] opined that, they are face-face, self-directed and teachable methods. According to [24], the delivery methods include conventional methods, Instructor-led and online methods. However, these methods have their individual downside when used alone. Consequently, we argue that, using all of them together will complement each other's deficiencies. Hence, the proposal for the use of the hybrid approach in delivering based on the peculiarity of the problem being addressed. The use of the hybrid approach will ensure that the weaknesses in each of the proposed traditional methods are complemented and compensated by the other method. This will lead to SEATE programs being effective and leads to improved security to social engineering attacks in particular and cybersecurity in general and SEATE programs in particular.

To propose a behavioural change artefact to improve SEATE programs, we propose a model known as Awareness, Transition, Adaptation and Consolidation (ATAC) following two theories (Conscious Competence Model and the stable Quasi-Random Equilibrium Model): [28],[22].

The CCM is a framework that describes the stages individuals have to pass through when learning a skills or behavior change to move from being unconscious/unskillful to becoming conscious/skillful. It is made up of four stages; Unconscious incompetence, where the individual as unaware, do not understand or know about a particular issue; in this case, SEATE programs and its impact. The second stage is Conscious Incompetence where the individual becomes aware of their skill/knowledge attitudinal deficit, hence, expresses the need to learn the skills or behavior change. At the third stage, called Conscious Competence, the individual have made progress and have acquired a reasonable level of the needed skill, but does things with little difficulty.

Finally, continuous use of the skill knowledge/ attitude over and over leads to Unconscious Competence where he/she performs the art/skill without thinking or with less effort.

The other theory is the stable quasi-stationary equilibrium, which describes change as a transition between two dynamic states in which each of the state itself is dynamic. It comprises unfreeze or unlock from present position to or behavior by creating an enabling environment through education training, motivation. The second is move from the present to the new state by implementing the new way of thinking or attitude. Thirdly; refreeze; by making the new system, the accepted way the system should work [22]. Consequently, following these principles/theories we argue that, the use of the ATAC model not only improve user SEATE knowledge/behavior, but will lead to permanent behavior/knowledge change and lead to permanent immunology among Users against Social Engineering Attacks. An Expert Opinion or Observational Empirical Research conducted showed very high rating for the metrics such as fit for purpose, novelty, ease of use and architecture/structure with 92% on average. This suggests that such a model has the potential to influence behavior change among users with overall average expert score of 73.6%.

VII. Conclusion and Future Work

The study aimed at Improving Social Engineering Awareness, Training and Education (SEATE) by exploring SEATE Content, Delivery methods, challenges and proposing an innovative Content, a hybrid Delivery method and a behavioral change model as a Non-Technical defense Approach to S E attacks defense.

The findings shows that SEATE fails due to poor content and poor delivery methods coupled with other challenges such as generic nature of training, limited budget provision, poor security policies and compliance and user resistance to changes. The use of relevant an innovative content, hybrid delivery methods, and a behavioral change model improves the conduct of SEATE programs.

As the cyber warfare in general and Social Engineering in particular rages on, with daunting challenges, cyber criminals have found innovative ways of penetrating the parametric defenses and delivering malicious content to users with the aim of compromising their systems. When that happens, the user becomes the last line of defense; to click or not to, update or not to. These critical binary decisions require that users understand the relevant SE Content conducted through well-delivered and innovative delivery methods. Consequently, following the novel model improves the immunity or resistance of users to SE attacks and enables them to know how to react in such attack circumstances. Thus, adopting the novel behavioral change model (ATAC) showed a high potential at improving the conduct of SEATE programs that improved user immunity/Resistance to SE attacks. One limitation of the model is the fact that, it was qualitatively evaluated; future effort will empirically follow the model to conduct a quantitative longitudinal study to practically establish the dimensions of the artefact (model) and to automate same for conduct of SEATE programs.

References

[1] Ahmed Alzarahni. Coronavirus Social Engineering Attacks: Issues and Recommendation. International Journal of Advanced Computer Science and Applications, Volume 11, No.5, 2020.

[2] Asma A. Alhashmi, Abdulbasit Darem, Jemal H. Abawajy. Taxonomy of Cybersecurity Awareness Delivery Methods: A Countermeasure for Phishing Threats. International Journal of Advanced Computer Science and Applications.Volume 12, No. 10, 2021.

[3] Symantec Security Summary. Covit 19 Attacks Continuo and New Threats on the rise. Symantec Enterprise Blogs, Retrieved, 20-12-21.

[4] Global Cybersecurity Index. Measuring Commitment to Cybersecurity. International Telecommunication Union, 2020.

[5] Hussein Aldawood, Geofrey Skinner. Reviewing cyber security Social Engineering Training and Awareness Programs-Pitfalls and Ongoing Issues. Future Internet, 2019. MDPI. https://doi: 10.3390/fi11030073.

[6] George Hatzivasilis, Soltiris Ioannidis, Micheal Smyrlis, George Spanoudakis, Fulvio Frati, Ludger Goeke, Torsten Hildebrandt, George Tsakirakis, Fotis Oikonomou, George Leftheriotis, and Hristo Koshutanski. Mordern Aspert of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees. Applied Sciences, 2020. Doi: 10.3390/app10165702.

[7] Fatima Salahdine & Naima Kaabouch (2019). Social Engineering Attacks: A survey. Future Internet, MDPI.doi.10.3390/fi11040089.

[8] Chritopher Hadnagy. Social Engineering: The Science of Human Hacking, Wiley, Indianapolise. URL: www.wiley.com, 2018.

[9] Sumar, Musah, Albladi, George, R.S. Weir. Predicting individuals' vulnerability to social engineering in social networks. Cybersecurity. Springer open, 2020. https://doi.org/101186/s42400-02-00047-5.

[10] Arroyo, A.M.,Rea,F.;Sandini, G.;Sciutti, A.Trust and social engineering in human robot interaction: will a robot make you disclose sensitive information, conform to its recommendation or gamble? IEEE Robot Autom. Lett.2018,3,3701-3708.

[11] David Airehrour, Nisha Vasudevan Nair, and SamanehMadanian . Social Engineering Attacks and Countermeasures. In the New Zealand Banking System: advancing a User-Reflective Mitigation, Information, and Austria. Information 2018,9(5), 110; https:// doi.org/10.3390/info9050110.

[12] Aldawood , H.; Skinner, G. Educating and raising awareness on cybersecurity social engineering: Aliterature Review . in proceedings of 2018 IEEE Internation Conference on Teaching, Assessment, and learning for engineering (TALE), Wollongong, NSW, Austria, 4-7 December 2018;pp.62-68.

[13] Albladi, S.M., Weir, R.S. Predicting individuals' vulnerability to social engineering in social entworks. Cybersecurity, springer open, 2020. https://doi.org/10.1186/s42400=020-00047-5.

[14] Albladi, S.M.;Weir,R.S. User characteristics that influence judgement of social engineering attacks in social networks. Human-centric computing and information sciences (2018). https://doi.org/10.1186/s13673-018-0128-7.

[15] Hussain, Hanizan Shaker; Din, Roshidi; Khidzir, Nik Zulkarnaen; Daud, Khairul Azhar; Ahmad, Suzastri . Risk and Threat via Online Social Network among Academia at Higher Education. International Conference on Big Data and Cloud Computing, 2019.

[16] Micalleff, N.; Arachchilage,N.A.G. involving users in the design of serious game for security questions education. arXiv preprint. ArXiv: 1710.03888, 2017.

[17] Soceanu, M. Vasylenko, and A. Gradianru "Improving Cybersecurity Skills Using Network Security Virtual Labs. "In Proceedings of the International Multi Conference of Engineers and Computer Scientists 2017 Vol II, IMECS.

[18] Merton Lansley, Francois Mouton, Stellios Kapetankis & Nikolaos Polatidis . SEADer ++: social Engineering attack detection in online environments using machine learning, Journal of information and Telecommunication,4:3, 346-362, 2020. doi:10.1080/24751839.202.174 7001.

[19] Nikolaos Tsinganos, Georgios Sakellarious, Panagiotis Fouliras, and IoannisMavridis . Towards an Automated Recognition System for Chatbased Social Engineering Attacks in Enterprise Environments. In ARES 2018: International Conference on Availability, Reliability and Security, August 27-30, 2018, Hamburg, Germany. ACM, ew York, NY USA, 10 pages.

[20] Mutlaq Alotaibi, Waleed Alfehaid. Information Security Awareness: A Review of Methods, challenges and Solutions.ICITST-WorldCIS-WCST-WCICSS-2018. Information Society. ISBN:978-1-908320-94-0.

[21] Ana Kovacevic, Sonja, D. Radenkovit. SAWIT: Security Awareness Improvement Tool in Workplace. Applied Sciences, 2020. MDPI. Doi: 10.3390/app10093065.

[22] Lewin, K. Field Theory in Social Science. Harper and Row: New York, 1951.

[23] Park, M., Oh,H., Lee, K. Security Risk Measurement for information leakage in IOT-based smart homes from situational awareness perspective. Sensors, 2019,19,2148Met al(2019).

[24] Abawajy, J. User preferences of cybersecurity awareness delivery methods," Behave. Inf. Technol, vol. 33, no. June 2015, pp-236-247, 2014.

[25] Ngqoyiyana, IL. Developing an Artefact for Raising S E Awareness among Administrative Staff. A Master of Science in Computer science. Dissertation (2020).

[26] Wieringa, R. Empirical Research Methods for Technology Validation: Scaling up to practice. Journal of system and Software (2013). Doi.org/10.1016/jss2013.11.1007.

[27] Vince, Reynolds. Social Engineering: The art of psychological warfare, human hacking, persuasion and deception (2015).

[28] Chapman, A. 2012. Conscious competence learning model: four stages of learning theory- unconscious incompetence, to conscious competence matrix-and other theories and models for learning and change. Businessball, Leiscester, UK. http://www.businessballs.com/consciouscompetencelearning model.htm.