Employee Awareness Model to Enhance Awareness of Social Engineering Threats in the Saudi Public Sector

Mohammed Fahad Alghenaim
Advanced Informatics Department
Razak Faculty of Technology and Informatics
Universiti Teknologi Malaysia
54100 Kuala Lumpur, Malaysia
aalghenaim@graduate.utm.my

Nur Azaliah Abu Bakar
Advanced Informatics Department
Razak Faculty of Technology and Informatics
Universiti Teknologi Malaysia
54100 Kuala Lumpur, Malaysia
azaliah@utm.my

Rasimah Che Mohd Yusoff
Advanced Informatics Department
Razak Faculty of Technology and Informatics
Universiti Teknologi Malaysia
54100 Kuala Lumpur, Malaysia
rasimah.kl@utm.my

Noor Hafizah Hassan
Advanced Informatics Department
Razak Faculty of Technology and Informatics
Universiti Teknologi Malaysia
54100 Kuala Lumpur, Malaysia
noorhafizah.kl@utm.my

Hasimi Sallehudin
Faculty of Information Science and Technology
Universiti Kebangsaan Malaysia
43600 Bangi, Malaysia
hasimi@ukm.edu.my

2021 International Congress of Advanced Technology and Engineering (ICOTEN) | 978-1-6654-1224-7/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICOTEN52080.2021.9493434

***Abstract*— The increase in social-engineering threats within the Saudi public sector has changed awareness and training methods. However, due to employees' lack of awareness, social engineering could lead to a breach whereby attackers identify vulnerabilities and subsequently launch their attacks. A social-engineering attack is a high risk to the Saudi public sector and may significantly affect its security measures. Thus, the benefits of adopting awareness-enhancement tools in the public sector are undeniable. This study proposes a conceptual awareness model designed to enhance employee awareness in the Saudi public sector to address this issue. This study reviews seven main factors of social engineering risk: phishing, baiting, pretexting, quid pro quo, tailgating, related security policies, and the ability to identify attacks and respond to threats. Additionally, this research examines one public sector actor in Saudi Arabia as a case study. The findings led to a model creation comprising of five components: a situation-awareness model for phishing, an information-security awareness tool, a power-knowledge-practice triangle, Saudi public sector follow-up metrics, and implementation phases. As a result, an a priori model was successfully developed, tested, and applied in the subsequent stage by the case study participants, the employees.**

Keywords*— *Awareness Model, Employee Awareness, Information Security, Saudi Public Sector, Social Engineering

I. INTRODUCTION

Criminals often use various forms of social engineering to identify their targets and prepare relevant instruments to attack them. At first, the method requires a malefactor to communicate with the target. Then, the perpetrators use social engineering to transfer malicious software to the victim. Social engineering differs from other forms of cyberattacks by transforming hacking into a form of social engineering. Put another way, when malefactors communicate with their targets using direct interaction, the internet, phone, or mobile applications, they may transform various forms of cyberattacks into forms of social engineering [1]. There are four significant social engineering steps: investigation, hook, play, and exit [2]. Social engineering is an instrument used to convince people to disclose their confidential data voluntarily to a malefactor [3, 4]. Some examples of such disclosures include sharing passwords, PINs, code words, and other information to provide critical data access. In addition to social engineering, malefactors may use malware to make their victims pay to restore the stolen information.

Despite the recent advancement of technology in the Saudi public sector, alarm concerning this sector's data security and privacy is rising due to its employees' security-awareness level. As the weakest link, employees represent the human factor that puts Saudi public-sector data at risk. Therefore, immediate action should be taken to ensure employees' and institutions' data are not jeopardised. Employees use technological solutions to assist with their daily operations. Thus, this paper assesses employees' awareness of social-engineering attacks by examining three variables and fourteen influential factors in the Saudi public sector; we thereby encourage a secure environment that complies with the existing security awareness indicators. Hence, comparative studies were conducted to analyse the related issues as well as prior studies of the Saudi public sector's security awareness, especially with regards to social engineering threats. Following this, the *employee awareness model for social engineering threats* will be proposed as a base principle to enhance employees' awareness of social-engineering attacks in a Saudi public environment.

II. RELATED WORKS IN SOCIAL ENGINEERING SECURITY

The diversity of technologies used in the public sector leads to many cybersecurity threats. This has forced regulators to tighten security measures from a technological, process-based, and people-based perspective. One of the critical security measures applied to the human aspect of public security is training in information security awareness. This includes formulating all necessary security-awareness models and related training tools and materials regarding cybersecurity and issues worldwide. In the following, we review three models related to the security awareness model, all of which have similar contexts to the scope of this study.

A. Shargawi's Situation Awareness Model for Phishing (SAMFP)

Shargawi's Situation Awareness Model for Phishing (SAMFP) is used in the e-learning sector and is one example of these security awareness models [5]. The SAMFP model offers a way to counter one of the most dangerous social-engineering attacks; phishing. SAMFP uses 16 human behavioural factors to test users' awareness of phishing attacks

978-1-6654-1224-7/21/$31.00 ©2021 IEEE

[5]. These factors, according to Shargawi, are temptation (e.g., greed), urgency or scarcity, over-confidence or self-consciousness, dispositional trust (e.g., over-trusting), authority, threats (or fear or anxiety), social proof, likability and similarity, reciprocation, curiosity (or excitement), commitment and consistency, overloading, diffusion of responsibility, showing off (e.g., heroism), convenience, and interpersonal relationships. As shown in Fig. 1, the SAMFP uses three levels to measure a user's improvement in awareness quantitatively: perception, comprehension, and projection.

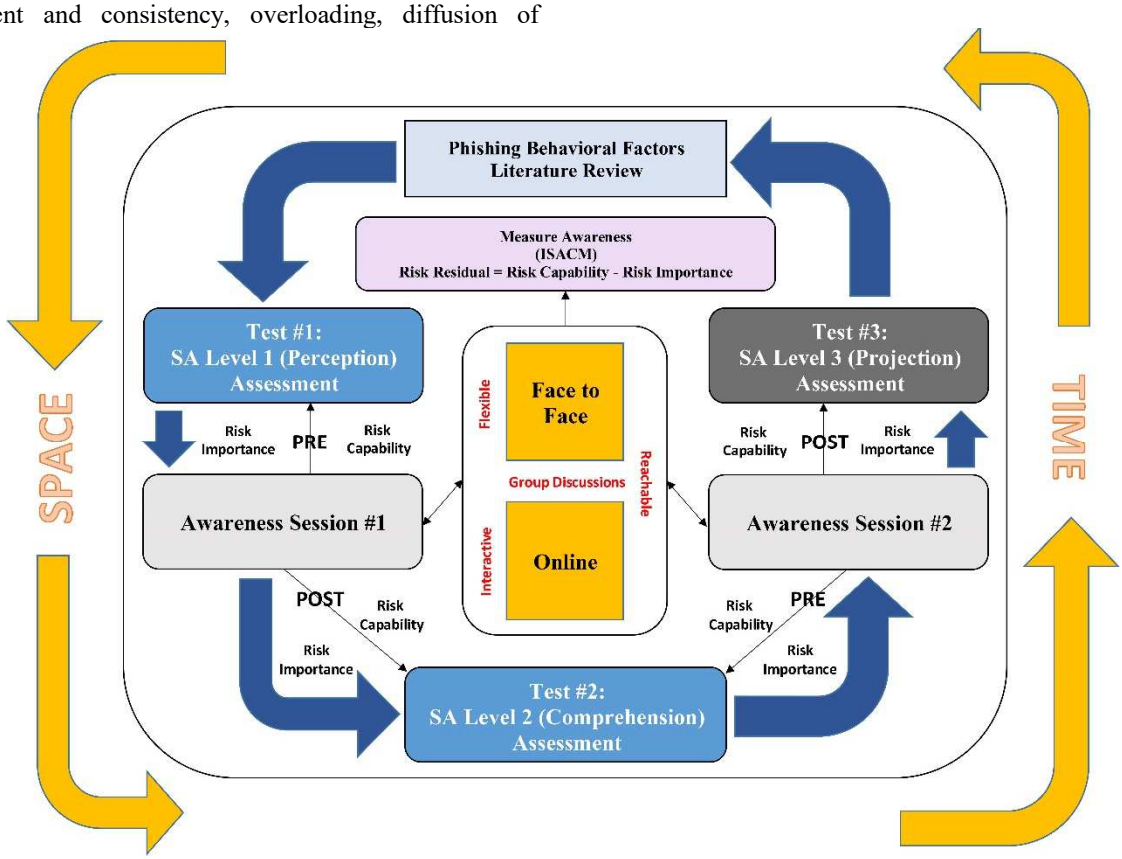

Fig. 1. Situation-awareness model for phishing (SAMFP)[5]

Shargawi's research aims to bolster awareness of phishing-related social engineering among participants and attain a satisfactory degree of protection. The SAMFP paradigm integrates instructive guidelines to promote competent, comprehensive, and interactive cognisance-delivery approaches for the study subjects, designed to realise heightened awareness. The guidelines include the following dimensions

- Reciprocal conversations, in contrast to unilateral communication, facilitate interactive participation by users.
- The development of measurable objectives to evaluate the awareness initiative's outcomes before and after the training activity.
- Malleable cognisance programs that can be modified to suit current needs or align with the assessment outcomes.
- Attainable programs include introducing communication approaches such as blogs, email, one-on-one and in-person presentations, wikis, and online surveys.

Shargawi embraced face-to-face discussions, wherein interlocutors employ a reciprocal and interactive philosophy [5]. This type of discussion aims to enhance partnership within the team. At the same time, its members deliberate on the progress of their awareness training. Furthermore, the awareness-delivery method involves online participants being organised into face-to-face groups. This way, the online arrangement includes the users who took part in the meetings using the web. Shargawi's analysis is custom-fitted to explore and assess the legitimacy of the mindfulness-conveyance approach as an influential space variable. The SAMFP measure is feasible and adaptable for addressing the circumstances of the investigation subject and includes the consideration of mindfulness levels and time regions. Therefore, the following section examines the execution of the interaction.

SAMFP is primarily influenced by the dynamic nature of the Situation Awareness Model (SAM) [1], which emphasises a dynamic approach to addressing and resolving awareness gaps and maintaining sustainability. Hence, its relationship with space and time offers awareness and sustainability in a continually changing field, such as information security. Notably, Shargawi's framework is a widely recommended guideline designed to increase awareness of the behavioural factors employed by users while engaging in phishing within online learning environments.

B. Situation-Awareness Model (SAM)

Endsley introduced the Situation-Awareness Model (SAM) as a systematic process in which additional awareness sessions increase awareness levels [1]. Situation awareness (SA) has always been critical to directing and executing

military infantry operations. By integrating and synthesising what is known about situation awareness (SA) in the infantry context, the results provide useful information for military developers and trainers. Engaging the enemy on urban or closed terrain and dealing with non-combatants, observers, and press members will add to the complexities and challenges of the tactical situation. The study discusses various measures and their advantages, disadvantages, and implementation considerations applied in simulation or field studies of new concepts and technologies. This study is designed to determine the discipline's advantages and disadvantages to ensure that problematic technologies are not adopted.

C. *Information Security Awareness Capability Model (ISACM)*

The SAMFP worldview accepts Poepjes' Information Security Awareness Capability Model (ISACM) [2] as it encourages and complements the quantitative assessment of the subjects' degrees of mindfulness, specifically related to phishing, at the three levels Endsley proposed. Fig. 2 depicts the idea of ISACM.

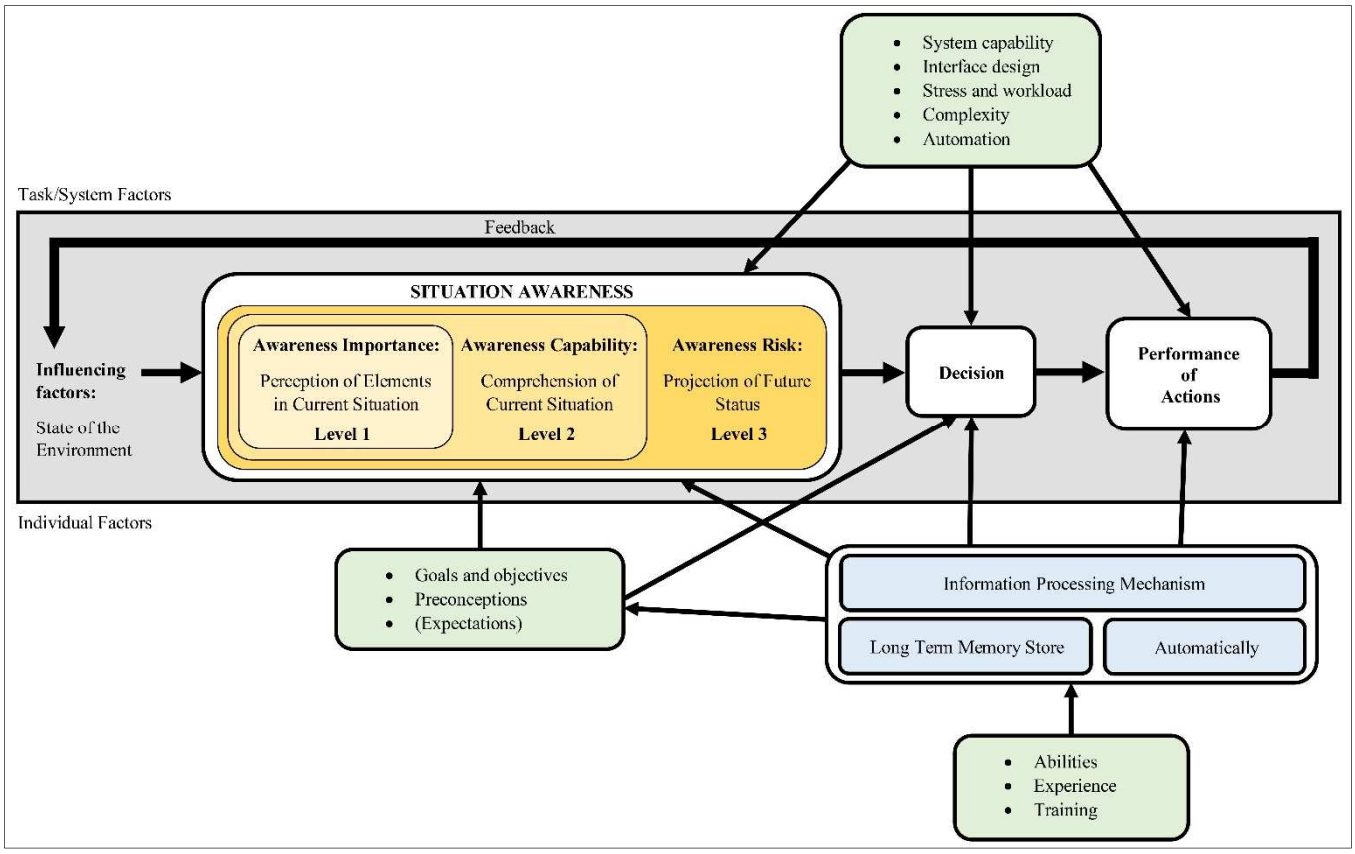

Fig. 2. Information Security Awareness Capability Model (ISACM)[7]

There are three levels of security awareness defined in this model. Level 1 is *perception*. Perception is considered the basis for understanding the position, characteristics, and changing aspects of germane environmental elements. In cyber-situational awareness testing, an employee's perceptiveness is considered the ground truth. In this primary stage, the examination assesses the level of members' comprehension of phishing. It also identifies the conduct that leads to phishing. Next is Level 2, *comprehension*. This level examines researchers' comprehension of pattern recognition, interpretation, and evaluation processes that come into play to synthesise disjointed Level 1 situation-awareness elements. This stage improves and evaluates a more profound comprehension of phishing and identifies the social causes that ensnare phishing victims. Finally is Level 3, *projection*. At this level, participants can predict how relevant elements in the environment will act in the future. This stage assesses the level of mindfulness among the members at the most significant level. The participants at this phase can predict phishing dangers by recognising conduct that leads to phishing.

D. *Comparison between the models*

Following disputes with SAMFP [3], researchers of SAM [1] and ISACM [8] indicated that the SAMFP worldview might misuse the two ISACM perspectives (*awareness* and *capability*) that inform SAM's third stage of assessment (awareness risk residuals). This criticism was based on subjects' scores on each of the three levels. So too was it based on the reported degree of difficulty faced by subjects on each of these test levels. Pre- and post-assessment tests encompass each of the three degrees of situational awareness in that capacity. However, the cyclical character of the SAMFP can portray the effects of the training's time variable, which encourages reiterated mindfulness periods. Furthermore, the SAMFP's adaptability trait is revealed by its use of the space variable, or its use of one-on-one, as well as online interaction methods, to cultivate mindfulness periods. Therefore, it is beyond doubt that the SAMFP accepts the two aforementioned factors and uses them to reinforce the manageability and progression of security mindfulness training presented to the investigation subjects.

From our analysis, we can conclude that SAMFP involves the following exceptional highlights. Firstly, the SAMFP uses joint feature sets present in one tool but absent in another. Secondly, the SAMFP embraces the best attributes from other individual fundamental learning paradigms and adds other distinct models to complement them. For instance, the model borrows the time and space elements from the SAM paradigm and improves them by integrating an innovative measurement technique to evaluate and monitor awareness-risk residuals and progress, as per the ISACM paradigm. The paradigm also fosters participants' continuous evaluation of the development of individual behavioural-awareness attributes after discrete tests. These evaluations help define the development of awareness materials to meet the appropriate participant-learning needs in the subsequent awareness cycles.

Thirdly, SAM and the ISACM paradigms failed to define the awareness development and conduct processes. In contrast, the proposed paradigm uses an instructive set of guidelines to steer the development and delivery of the awareness initiative. The model further ascertains whether subjects continue to evaluate their degree of awareness of the individual-level behaviours that create security risks. The obtained information can also help define the focus for developing appropriate awareness based on the participants' learning needs during the high-cognisance periods of the awareness cycle. The paradigm introduces a periodic review to document risky behavioural attributes and provide employees with new information, thereby facilitating the model's relevance and timeliness.

Our findings also indicate that Shargawi mentioned embedding online information-awareness tools (game-based approaches) in training to help users enhance their awareness process. These tools are experimental and require control groups to monitor the before-and-after effects to evaluate the proposed program's efficiency [3]. Furthermore, these tools are highly effective because they simulate the conditions of an actual phishing attack. Shargawi has discussed the effectiveness of these awareness tools (PhishGuru, Anti-Phish Phil, Phree of Phish, PhishMe, GoPhish, and Phishing IQ) and their ability to enhance employees' security awareness. However, these online awareness tools have the following disadvantages, as highlighted by other studies, which are:

- They focus only on phishing attacks [4–6].
- They do not address security policies related to social engineering threats used by each institution [7–10].
- Foreign companies and organisations own these tools [5, 11–14].
- They use the internet to deliver awareness assessment and enhancement services [11, 15, 16].

Therefore, this paper aims to propose a conceptual framework referred to as the Employee Awareness Model for Social Engineering Threats (EAMSET); a localised tool in the public sector environment that aims to leverage the existing advantages of these existing security awareness models and must yet be able to resolve the weaknesses existing within the previous models.

III. Research Methodology

An exploratory sequential methodology supported with mixed-method open-end employee questionnaires is used to evaluate the proposed model. ISAT is to be evaluated three times, once every two months, in a continuous cycle using the tool's reports to determine the tool's effectiveness. Following this is the design stage, which involves defining the research unit, classifying the anticipated study's fundamental problems, and designing procedures for maintaining case study consistency. The Ministry of Foreign Affairs of the Kingdom of Saudi Arabia is chosen as a case study. It is one of the leading government industries and is a critical developer of several pilot deployment programs ranging from data protection to technical infrastructure. This ministry is divided into many branches, including protected data departments, information technology support centres, information department, training and policy studies. The ministry upholds its service delivery requirements by adhering to Saudi national security. As shown in Fig. 3, the proposed model is based on the power-knowledge-practice triangle methodology; power (Follow-Up Indicators), knowledge (adopting new training methods), and practice (ensure the continuation of the training process) [26]. Follow-Up Indicators for the Saudi Public Sector (SPSFUIs) include proposals for strategy training, workforce responsibility, employee retention, and assistance from accountable departments.

Later in the planning stage, the process would focus on improving all case study investigators' skills, then creating a case study procedure, performing a pilot case, and obtaining all necessary approvals. In preparation for this, and to ensure the study's reliability, a case study protocol was created. Furthermore, since one of the author's works for a ministry and the research focuses only on technology without involving any government or employee results, the author can obtain permission for the study to proceed without dispute.

The stage following this is the selection stage, which entails following a case study procedure and using various sources of information, creating a case study database, and retaining a chain of evidence. In preparing the case study, the author has already undertaken a series of semi-structured interviews with Ministry IT officers and information technology experts to understand better the ministry's activities and current state of security implementation. The objective is to understand better the present state of training delivery and potential security threats. The stage following this studies secondary scientific propositions and other techniques to investigate alternative theories and hypotheses for the results.

As a result, explanation building analysis is used because it can analyse case study evidence and can explain the case. Finally, there is the stage of sharing. The textual, instrument-based, and visual resources are designed to illustrate the analysis's facts. The final output of this analysis is to put forward a proposal for the Employee Awareness Model for Social Engineering Threats (EAMSET) that is tailored specifically to the KSA public sector.

IV. Formulation of the Employee Awareness Model for Social Engineering Threats

In formulating a new Employee Awareness Model for Social Engineering Threats (EAMSET), this study considers the components from SAMFP, ESAM, ISACM, and the Saudi public sector's follow-up indicators such as plans for strategy training accountability, employee satisfaction, and responsible department's support. EAMSET aims to improve the level of employees' awareness and knowledge of security, particularly social-engineering threats.

EAMSET is not limited to SAMFP components, factors, and phishing attacks only. Instead, EAMSET includes more components, factors, and variables with more stringent and up-to-date requirements to successfully conform to the Saudi public sector's proposed framework. Nevertheless, all of the factors associated with EAMSET are localised inside the institutions, except for sharing security-related information among employees through online domains. As mentioned earlier, EAMSET adopts Shargawi's model [5]; however, EAMSET does not merely focus on the SAMFP's 16 human factors. Instead, EAMSET uses different factors, sub-factors, and variables to assess and enhance the awareness of the five types of social-engineering threats, namely phishing, baiting, pretexting, quid pro quo, and tailgating; this new model EAMSET also provides the security policies with the ability to identify attacks and respond to threats. Fig. 3 shows the added components, factors, sub-factors, and variables in EAMSET marked with a dotted line.

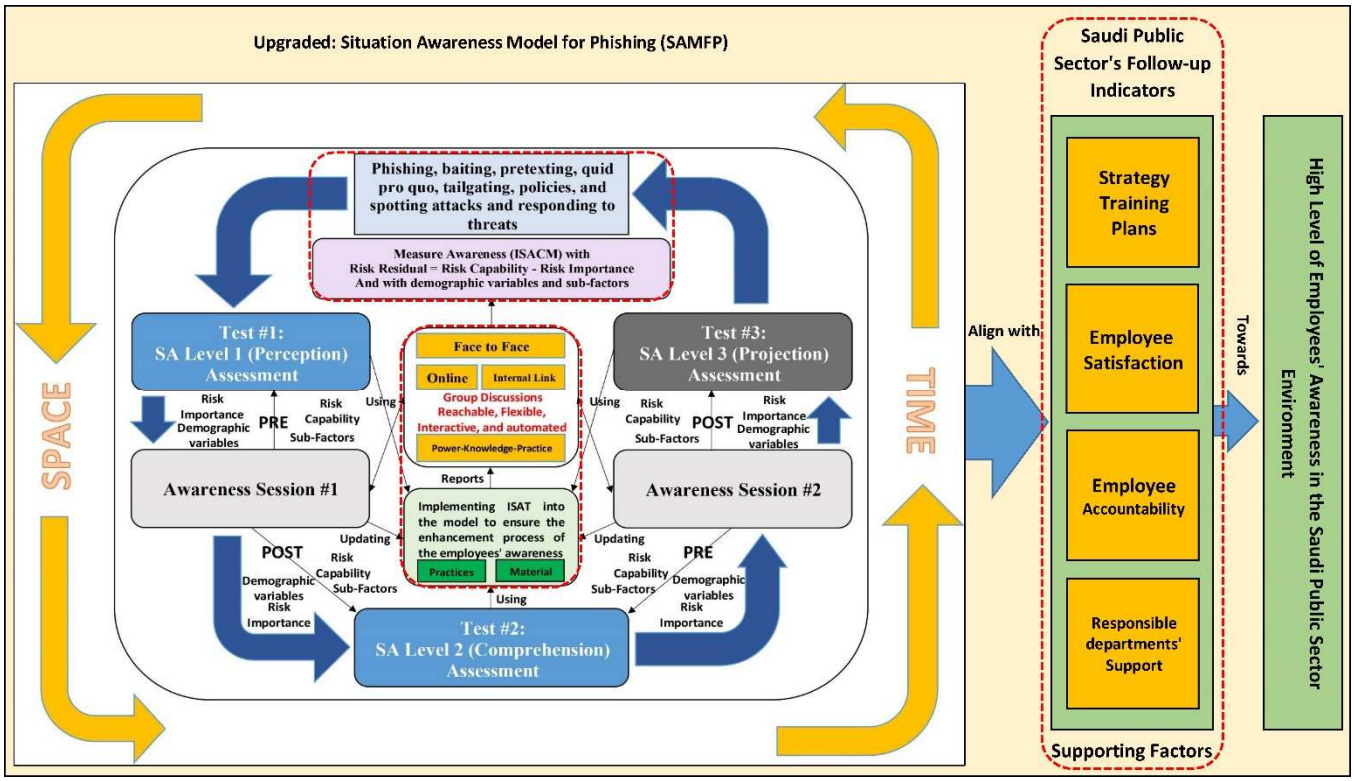

Fig. 3. The proposed employee awareness model for social engineering threats.

Based on the KSA public sector requirement for combating social engineering threats, six additional threats are included in EAMSET: pretexting, baiting, tailgating, quid pro quo, related security policies, and the ability to identify attacks and respond to threats. This model also includes the element of "power-knowledge-practice" as the principle for handling such threats. Besides this, this new model also includes ISACM components, including practices and materials.

EAMSET also included the four main factors of Saudi Public Sector Follow-Up Indicator (SPSFUI): first, **Strategy training plans**: Social-engineering-awareness training strategies are essential for providing practical knowledge to protect corporate assets. This is strongly supported by many studies that indicate the methods used to make these training sessions work are not essential because employee engagement serves as a much more important variable owed managerial consideration [7, 17–20]. The threats posed by social engineering are nothing but a response to technological development and human error.

Second is **Employee satisfaction**: Security is deeply embedded in an organisational culture that emphasises employee satisfaction. The training efforts must consider employee satisfaction as an essential variable. As stated by many studies, the quality and usability of training tools and programs can increase employee satisfaction. Using digital tools can also enhance satisfaction and reduce employee errors [21–23].

The third is **Employee accountability**: Holding employees accountable for understanding the provided security training is essential for enhancing the Saudi public sector's awareness of cybersecurity and social-engineering threats. Other researchers strongly support the notion that robust security-awareness programs should be integrated with relevant training to improve the cybersecurity approach [9, 20, 24].

Finally, the fourth factor is the **Responsible department's support**: Enhancing employees' awareness of cybersecurity threats is essential to improving security. Senior management's responsibilities should revolve around managing various resources, employing digital security, and promoting cybersecurity values among less-trained employees. Moreover, security program managers must enhance awareness among employees to strengthen security [20, 25].

V. CONCLUSION

The goals of the Saudi public sector's security awareness model are to evaluate and strengthen employees' awareness of social engineering risks, to improve the standard of preparation, and to minimise risk costs. This is possible if

EAMSET is implemented successfully and securely. EAMSET shall develop universally agreed-upon standards, procedures, tools, and models to assist all Saudi public sector practitioners to increase their efficacy and value. Employee awareness, public sector awareness, and an adequate supportive information security system contribute to the practical or rapid and smooth implementation of the awareness model in the Saudi public sector. For future work, this model will be tested by information security specialists based on the proposed components' relevance and their viability and usefulness by Saudi public practitioners

ACKNOWLEDGMENT

This work is supported by Universiti Teknologi Malaysia with cost center number Q.K130000.2656.17J22.

REFERENCES

[1] M. R. Endsley, "Final reflections: situation awareness models and measures," Journal of Cognitive Engineering and Decision Making, vol. 9, no. 1, pp. 101–111, 2015.

[2] F. Breda, H. Barbosa, and T. Morais, "Social engineering and cybersecurity," in 2017 11th International Technology, Education and Development Conference, 2017, pp. 4204–4211: IEEE.

[3] A. Shargawi, "Understanding the human behavioural factors behind online learners' susceptibility to phishing attacks," Lancaster University, 2017.

[4] A. Koyun and E. Al Janabi, "Social engineering attacks," Journal of Multidisciplinary Engineering Science and Technology (JMEST), vol. 4, no. 6, pp. 7533–7538, 2017.

[5] J. W. H. Bullée, L. Montoya, W. Pieters, M. Junger, and P. Hartel, "On the anatomy of social engineering attacks−A literature - based dissection of successful attacks," Journal of investigative psychology and offender profiling, vol. 15, no. 1, pp. 20–45, 2018.

[6] M. Junger, L. Montoya, and F.-J. Overink, "Priming and warnings are not effective to prevent social engineering attacks," Computers in human behavior, vol. 66, pp. 75–87, 2017.

[7] H. Aldawood and G. Skinner, "Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues," Future Internet, vol. 11, no. 3, p. 73, 2019.

[8] H. Aldawood and G. Skinner, "Challenges of implementing training and awareness programs targeting cyber security social engineering," in 2019 Cybersecurity and Cyberforensics Conference (CCC), 2019, pp. 111–117: IEEE.

[9] M. J. Miranda, "Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach," International Management Review, vol. 14, no. 2, pp. 5–10, 2018.

[10] I. Ghafir et al., "Security threats to critical infrastructure: the human factor," The Journal of Supercomputing, vol. 74, no. 10, pp. 4986–5002, 2018.

[11] A. E. Juncos, "Resilience as the new EU foreign policy paradigm: a pragmatist turn?," European security, vol. 26, no. 1, pp. 1–18, 2017.

[12] K. Tokas and K. Yadav, "Foreign ownership and corporate social responsibility: The case of an emerging market," Global Business Review, p. 0972150920920444, 2020.

[13] S. M. Albladi and G. R. Weir, "User characteristics that influence judgment of social engineering attacks in social networks," Human-centric Computing and Information Sciences, vol. 8, no. 1, pp. 1–24, 2018.

[14] M. Bossetta, "The weaponisation of social media: Spear phishing and cyberattacks on democracy," Journal of international affairs, vol. 71, no. 1.5, pp. 97–106, 2018.

[15] L. Xiangyu, L. Qiuyang, and S. Chandel, "Social engineering and insider threats," in 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2017, pp. 25–34: IEEE.

[16] P. Vadrevu and R. Perdisci, "What you see is not what you get: Discovering and tracking social engineering attack campaigns," in Proceedings of the Internet Measurement Conference, 2019, pp. 308–321.

[17] J. M. Hatfield, "Social engineering in cybersecurity: The evolution of a concept," Computers & Security, vol. 73, pp. 102–113, 2018.

[18] A. Rege, T. Nguyen, and R. Bleiman, "A social engineering awareness and training workshop for STEM students and practitioners," in 2020 IEEE Integrated STEM Education Conference (ISEC), 2020, pp. 1–6: IEEE.

[19] H. Aldawood and G. Skinner, "Educating and raising awareness on cyber security social engineering: A literature review," in 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), 2018, pp. 62–68: IEEE.

[20] F. Salahdine and N. Kaabouch, "Social engineering attacks: a survey," Future Internet, vol. 11, no. 4, p. 89, 2019.

[21] W. Fan, K. Lwakatare, and R. Rong, "Social engineering: IE based model of human weakness for attack and defense investigations," International Journal of Computer Network & Information Security, vol. 9, no. 1, 2017.

[22] I. G. P. Kawiana, L. K. C. Dewi, L. K. B. Martini, and I. B. R. Suardana, "The influence of organisational culture, employee satisfaction, personality, and organisational commitment towards employee performance," International research journal of management, IT and social sciences, vol. 5, no. 3, pp. 35–45, 2018.

[23] T. Bakhshi, "Social engineering: revisiting end-user awareness and susceptibility to classic attack vectors," in 2017 13th International Conference on Emerging Technologies (ICET), 2017, pp. 1–6: IEEE.

[24] A. Caballero, "Security education, training, and awareness," in Computer and information security handbook: Elsevier, 2017, pp. 497–505.

[25] M. Edwards, R. Larson, B. Green, A. Rashid, and A. Baron, "Panning for gold: Automatically analysing online social engineering attack surfaces," computers & security, vol. 69, pp. 18–34, 2017.

[26] D. King and J. Hayes, "The effects of power relationships: knowledge, practice and a new form of regulatory capture," Journal of Risk Research, vol. 21, no. 9, pp. 1104–1116, 2018.