IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 27 November 2022, accepted 10 December 2022, date of publication 16 December 2022,
date of current version 22 December 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3230286

RESEARCH ARTICLE

Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior

BADER ALKHAZI[1], MONEER ALSHAIKH[2], SULAIMAN ALKHEZI[3], AND HAMZA LABBACI[4]

[1]Department of Information Science, College of Life Sciences, Kuwait University, Safat 13060, Kuwait
[2]Department of Cybersecurity, College of Computer Science and Engineering, University of Jeddah, Jeddah 23218, Saudi Arabia
[3]Computer Science Department, College of Science, Kuwait University, Safat 13060, Kuwait
[4]Department of Computer Science, University of Tours, 37200 Tours, France

Corresponding author: Bader Alkhazi (bader.alkhazi@ku.edu.kw)

This work involved human subjects or animals in its research. Approval of all ethical and experimental procedures and protocols was granted by the Ethics Review Committee (ERC), Kuwait University.

ABSTRACT Technology is changing the way we work more than ever before. Therefore, it is critical to understand the security threats associated with these advanced tools to protect systems and data. Security is a combination of people, processes, and technology. Thus, to effectively counter cyber-threats, information security awareness (ISA) programs are an essential cornerstone of enterprise security. There are many ways in which information security knowledge can be delivered. In this paper, we have conducted an experiment to test the impact of multiple intervention strategies on knowledge, attitude, and behavior. The HAIS-Q was used to evaluate the effectiveness of training methods on the employees. Our study suggests that all methods raise knowledge equivalently. However, having more than one delivery method to convey the same message has a greater impact on users' attitudes. When it comes to behavioral change, however, text-based and game-based training formats performed better than their counterparts. Additionally, employees' tendency to engage in self-education activities and participate in future awareness programs was influenced by the intervention strategy. These findings have important implications, as ISA programs should be designed in a way that positively influences the mindset of employees and motivates them to embrace security practices in their daily activities.

INDEX TERMS Information security awareness, security training, security management, cybersecurity, cybersecurity assessment.

I. INTRODUCTION

Information technology (IT) surrounds all elements of our lives. In a very short period, technology has become the cornerstone for the development of many critical areas such as health, transportation, business administration and education. Both private organizations and government agencies have embraced technology and connected their key assets to the internet to improve services and maintain their competitive advantages. In order for government agencies and private companies to protect their IT infrastructure and data, they have increased their focus on technology-based security measures, neglecting the fact that effective security is a combination of people, processes, and technology. Thus, large organizations which have invested heavily in strong security technologies have continuously reported security incidents [33], [35].

Many studies have reported that the human factor is the weakest link in the security chain [1], [9], [26], [78]. For instance, [42] reported that 46% of cyber-security cases in the last year were due careless or uninformed staff. Other security service providers have reported similar results [31], [77].

The associate editor coordinating the review of this manuscript and approving it for publication was Liang-Bi Chen.

A number of studies have suggested that awareness training is the most effective approach in preventing these attacks [6], [8], [12], [63], as users are the final line of defense against many cyber-threats. For this reason, organizations should not only be concerned with technological solutions but should also address human vulnerabilities and invest in raising cyber-security awareness [11], [67].

One of the important measures to increase the degree of security is by awareness training. Previous research reported that only a third of Information Security Awareness (ISA) programs are effective [18]. Unsuccessful cybersecurity training leads to higher anticipation costs without reducing failure cost [53], [59], driving the total cybersecurity investment cost up. Therefore, it is important to study how to conduct an effective training program. To do so, there are two important factors to be considered [83]: the up-to-date relevant knowledge and the intervention strategy. The training program needs to be designed in a way that not only improve knowledge, but should also motivate employees to build good habits [8], [10]. Previous studies adopted the Knowledge Attitude Behavior (KAB) model to measure Information Security Awareness (ISA) programs [44]. The core concept of KAB is that more knowledge about security procedures and policies leads to an improvement in attitude towards their importance, which ultimately enhances security-related behavior.

In this paper, we investigate and compare the impact of different ISA delivery methods on public sector employees' knowledge, attitudes, and behaviors. We use in our study the Human Aspects of Information Security Questionnaire (HAIS-Q) [55], which is based on the KAB model, as a measurement instrument for users' ISA. Furthermore, we compare users' feedback on four intervention methods. Our results show that different training methods are able to raise employee's knowledge equally. However, attending more than one training format significantly improves employees' attitudes and behaviors compared to those who attend only a lecture. Furthermore, results indicate that participants who find the training program enjoyable and engaging are less likely to suffer from security fatigue [6], [54]. Also, they are more likely to take part in self-development activities such as voluntarily participating in future awareness campaigns. In fact, a successful training program motivates participants to engage with other employees regarding the content of the program, improving peer interaction and knowledge sharing. Finally, participants are more likely to stay committed during the entire program, leading to a more secure organization.

The remainder of this paper is structured as follows. We first introduce the required theoretical background and related work in section II and III, respectively. Our methodology is described in section IV. Results and the threats to validity are in section V and section VI, respectively. Followed by the discussion and implications in section VII. Finally, in section VIII, we summarize and present ideas for future work.

II. BACKGROUND

There is a wide consensus throughout the literature concerning the need for organizations to develop SETA programs on incidents related to the human factor [4], [12]. Existing information security management frameworks and standards integrate SETA with other key security functions such as security policy, risk management, and incident management [4], [9], [10].

The literature distinguished the different roles of education, training, and awareness. [80] suggest: Education is where security professionals integrate security skills and competencies into a common body of knowledge for the design and implementation of information security; Training is where relevant employees gain needed security skills and competency around security to enable them to perform their job; Awareness involves focusing all other employees' attention on security, giving them the ability to avoid behaviors that would compromise information security. Most organizations when applying SETA programs only implement awareness for employees and education, and training was conducted by external providers for individual personnel where required. From this point on, we subsequently use the term information security awareness (ISA) instead of SETA.

The importance of ISA programs in safeguarding information assets has compelled many authors to recommend their use within organizations as part of their overall security strategy [12], [23], [52]. There exist several guidelines for organizations developing ISA programs [11], which can be broken down into three fundamental phases: (1) development, (2) implementation, and (3) evaluation. The following discussion uses them to review existing approaches and models for developing ISA programs.

The development phase includes activities used to understand the current organizational situation, obtain management support, and acquire the resources necessary to develop an effective program [9], [16]. These activities involve conducting a needs assessment for an ISA program, which contain legislated requirements, defining goals and objectives, establishing the ISA development team, and identifying the target audience for an ISA program [47]. The literature highlighted the importance of understanding the needs of an organization and its culture and the design of ISA programs that meets these specific needs [81]. For instance, [16] suggest that security awareness should be professionally prepared and organized for it to work and needs to be targeted and actionable. Development phase activities also include developing materials for ISA consisting of tasks around topic selection and material creation [23], [86].

The implementation phase focuses on the conduct of the ISA program using a variety of delivery methods. The literature on the implementation of ISA programs discussed methods for effectively delivering ISA messages. These include the use of a combination thereof such as newsletters, emails, note-taking tools to aid memory (e.g., pens and notepads), and posters exposing suspects within the organization

via security messages on a consistent and ongoing basis [1], [23].

The final ISA phase is evaluation, where the organization reviews and evaluates its ISA initiatives to measure their effectiveness. This is typically performed by identifying changes in employee behavior that impact information security [68]. Existing approaches focus on an exceedingly limiting view of gauging the data obtained by the program. Also, discussion about the evaluation of ISA programs largely focus on the outcome, which was raising employees' awareness [11], [24], [30], but notably overlook assessing the practices themselves as well as the overall approach to the development of ISA in organizations. Evaluation should instead focus on the effect of ISA holds on overall security due to the changes in employee behavior [68]. One way to measure the effectiveness of ISA is to compare the incidence of noncompliance-related security events before and after implementation of the ISA program.

Best-practice standards such as [40] stress the need for ISA programs, recommending that ''all employees of the organization should receive appropriate awareness, education, and training and regular updates in organizational policies and procedures, as relevant for their job function.'' However, the standards neglect to provide clear and practical guidance on ISA program implementation and effective methods for changing employees' behavior. Standard advice lacks support from empirical data and pays little consideration to organizational context [13], [30], [66]. Therefore, there exists a need to find empirical evidence via experimental research to assist organizations in finding the proper ISA methods needed to raise their employees' awareness and ultimately change their security behavior.

III. RELATED WORK

A. SECURITY AWARENESS METHODS

Regarding the contribution of this paper, there have been efforts to compare awareness training methods for different objectives. For instance, [75] investigated user preferences for and effectiveness of security awareness training methodologies in Thailand. In this study, the students were divided into two groups, and each group received a combination of instructor-led, video-based, text-based and game-based training sessions on phishing. The participants received pre- and post-training questionnaires to collect their opinions and to study their improvements in awareness. Moreover, the researchers sent multiple stimuli phishing emails before and after the training to study the improvement in users' abilities to distinguish between phishing and legitimate emails. The authors concluded that the training is successful in raising user confidence and in decreasing the false-negative rate, although the false-positive results remained unchanged. Additionally, the users did not prefer any particular sequence of training methods over the other, but most of the participants preferred the traditional classroom-based training when asked to identify one delivery method of choice.

Another example is the work of [72]. In this study, the authors investigated four aspects of each training delivery method: effectiveness, user satisfaction, confidence, and time-efficiency. The experiment mainly focused on phishing awareness using three delivery formats: text-based, instructor-based and computer-based training. The authors chose school students to conduct the experiments, to make sure that the participants were homogeneous in terms of sociodemographic factors. They concluded that instructor-based training was best in terms of user satisfaction, effectiveness and increasing confidence. However, the value for time was the lowest. In contrast, when time was the most pressing matter, text-based training was the most efficient, despite its lower performance in the three other aspects.

In [1], the author's objective was to determine which awareness delivery method is best for increasing cybersecurity awareness levels, and which one is preferred by users. The study divided participants into six groups. Three groups took only one awareness session about phishing, either text-based, video-based, or game-based; the other three groups took all three sessions in different orders. Although the participants preferred the video presentation session, the groups that attended mixed training delivery methods learned more information about the topic.

[32] performed a pilot study to evaluate the influence of simulation video games on knowledge transfer regarding information security concepts such as social engineering, firewall policies, the use of Secure Shell Protocol (SSH), and physical security. Sixteen (16) university students from Thailand were selected and divided into two groups of eight. One group played the CyberCIEGE video game, while the other attended a traditional instructor-led training session for one hour. The results showed that the participants enjoyed the game and indicated that it is more mentally challenging. Also, those who completed the game demonstrated a knowledge increase and an understanding of most of the covered topic. However, not all participants completed the game since some claimed that they got bored, faced technical difficulties, or a language barrier.

Finally, the authors in [65] classified security awareness into three levels: perception, comprehension, and projection. Level 1 (perception) is basically the ability to understand the presence of a threat. When someone reaches the next level (comprehension), they will be able to integrate and interpret information from multiple sources properly. Finally, projection means that users are able to predict potential security risks, enabling them to handle risks correctly. The participants in this study were 153 freshmen from a private university in Taiwan. They were evenly assigned into three groups, and each group received either hypertext-based security awareness training, multimedia-based security awareness training, or hypermedia-based security awareness training. The results of this study demonstrated that hypermedia-based and multimedia-based training are not very effective at introducing a new subject to users, since it may divert learners'

attention from the materials. Thus hypertext-based training is better at raising user perception of security threats. However, when it comes to stepping up the ladder to comprehension and projection levels, multimedia-based training outperformed hypertext-based security awareness training. Moreover, students who attended hypermedia-based sessions performed better than those who attended multimedia-based training on all three security awareness levels.

To summarize, while prior research has studied different aspects and characteristics of training methods, they were conducted in an isolated manner. Furthermore, most of the work was directed towards students and tackled one particular component of information security awareness, namely email management or phishing. In our field study, we used a holistic ISA, consisting of seven focus areas to analyze the impact of various intervention techniques on working employees.

B. SECURITY AWARENESS ASSESSMENT

Most organizations have several cyber resilience goals with an objective to provide their services under all circumstances. An employee unprepared for cyber risks could expose the organization to numerous cyber-attacks. Thus, decision-makers are interested in investigating risk causes and sources to take preventive measures accordingly. Few commercial organizations publish annual surveys concerning security breaches [22], [27], [73]. These reports often concern themselves with the impact of these risks as opposed to the opinions of employees on security-related issues. In fact, their methodology, questions design, analysis, and motivation have been criticized by several researchers [36], [39], [55]. To compensate, a growing number of researchers developed survey-based methodologies to understand or assess individual security levels [2]. The main limitation of these approaches is their focus on one narrow area. For instance, the authors in [50] and [20] were only concerned about mobile devices security. Other reports focused on phishing threats [14] or social media-related issues [3], [76]. References [57] and [56] both attempted to propose a comprehensive measurement tool of the overall ISA of employees and to formalize the conceptual development of the Human Aspects of Information Security Questionnaire questionnaire (HAIS-Q), its initial reliability, and validity testing.

HAIS-Q was used and validated in a respectable number of empirical studies in the ISA field. For example, [56] used HAIS-Q to examine the link between knowledge about policies and behavior when using work computers. A study to test the construct validity of the HAIS-Q was presented in the reports of [55]. while the authors conducted a lab-based study, its objective was to only find out whether the questionnaire can predict user's behavior based on their responses. A closely related study by [48] investigated whether personality traits (e.g., agreeableness, conscientiousness, emotional stability, and risk-taking propensity) could be linked with better information security policies and procedures. In fact, [58] argued that considering user learning styles in training design could improve information security awareness. In both studies, however, participants failed to receive similar training packages in terms of content and frequency. Moreover, the studies did not measure the influence of matching styles directly. They instead reported a connection between learning styles and ISA. *While previous studies sought to examine the current users' security awareness levels, our objective is to empirically test the impact of the different training strategies on users' knowledge, attitude, and behavior. Furthermore, our work is based on a controlled experiment where participants were carefully assigned to groups to minimize the knowledge gap and demographic effect.*

TABLE 1. Participants' information.

Variables	Frequency	Percentage
Gender		
Male	63	49.22%
Female	65	18.75%
Age Group		
18-24	35	27.34%
25-30	24	18.75%
31-40	43	33.59%
41-50	21	16.41%
Above 50	5	3.91%
Education		
Diploma	38	29.69%
Bachelor	50	39.06%
Master	25	19.53%
PhD	15	11.72%
Position		
Entry level	52	40.63%
Mid-level	47	36.72%
Higher Management	29	22.66%
Length of Service (years)		
<5	24	18.75%
5 - 10	29	22.66%
11 - 15	30	23.44%
16 - 20	13	10.16%
21 - 25	17	13.28%
Above 25	15	11.72%

IV. METHODOLOGY

We performed a user study and defined four research questions that address the effectiveness, suitability, and enjoyment of the training approaches. Every training campaign has an objective: some simply aim to increase people's awareness of an issue, while others require an action. Choosing the right way to convey the message will help accomplishing the target goal efficiently. Thus, we investigate the corresponding effect each delivery method has on knowledge, attitude, and behavior.

- **RQ1: What is the impact of every training method on knowledge acquisition?** The first step in the KAB model is knowledge. It helps in understanding, familiarizing, or being aware of something. There are multiple ways in which we can inform users about cyber-security

topics. This question investigates the amount of change in users' knowledge caused by the different intervention strategies.

- **RQ2: How are the attitudes of users affected by each intervention approach?** Attitude refers to the state of mind an individual has about the object of interest [62], and it is directly linked with their awareness level [15], [49]. In this research question, we would like to examine the effect of each training technique on the amount of attitude change towards security concepts.
- **RQ3: Is there a relation between behavioral change and the way we train employees?** The ultimate objective of Information Security Awareness (ISA) programs is not only to educate employees about the importance and implications of security policies, but also to behave in accordance to these rules and guidelines [44]. The KAB model suggests that behavior transformation is gradual, it is the result of knowledge accumulation that initiates an attitude change over some period of time. Thus, in this question, we would like to study the influence each training method has on employees' behavior.
- **RQ4: How satisfied are employees with each training experience?** Cyber-security threats are complex and evolve rapidly; thus, most awareness training campaigns are performed periodically to keep the security policies fresh in the employees' minds, which helps keep both users and systems safe. We would like to acquire the participants' feedback on the training process and see how it correlates with knowledge, behaviors, and attitudes. Moreover, enjoying a training experience will reduce the failure cost and may potentially encourage future self-learning, which will lead to a more secure organization [59].

A. RECRUITMENT

This study involved 140 voluntary participants representing 12 job areas from four different government bodies in Kuwait concerning education, health care, services, and infrastructure. All respondents are working either in a part-time or a full-time job, and they all reported that they use computers or mobile devices at work. Each participant completed a short information questionnaire to obtain general information about their age, gender, education, position, languages, and other factors to reduce potential demographic effects between the groups. Kuwait National IT Governance Framework (KNIGF) mandates that all new information system users (including third-party users and contractors) should be provided with basic security awareness training. Moreover, specialized role-based training is performed before authorizing access to IT assets or when major changes emerge in information systems or operation environment. Thus, all participants attended at least one basic security training before this experiment. Only 128 participants completed the study until the end, so we excluded those who did not continue from our analysis. The age of our sample ranges from 18-57. 63 are males (49.2%) and 65 are females (50.7%). Participants were divided into three job levels: executive level (22.6%), mid-level (36.7%), and entry level (40.6%). The participants' computer experience ranges from seven to 35 years, and the average time spent on electronic devices daily is 3.3 hours, Table 1 shows a summary of the participants' information.

TABLE 2. Groups details.

Group	Treatment	Participants	Male	Female
A	Lecture + Video	33	15	18
B	Lecture + Reading	32	18	14
C	Lecture + Game	32	16	16
D	Lecture Only	31	14	17
	TOTAL	128	63	65

B. THE HUMAN ASPECTS OF INFORMATION SECURITY MODEL

HAIS-Q is an instrument based on the KAB model to measure information security awareness. An overview of HAIS-Q is shown in Figure 1. There exist seven areas of interest: email and internet use, password management, social media use, incident reporting, information handling, and mobile computing. For every focus area, there are three sub-areas, each of which has one knowledge statement, one attitude statement, and one behavior statement. For instance, the following statements are an example of the password management focus area [55]:

Knowledge: "It's acceptable to use my social media passwords on my work account."

Attitude: "It's safe to use the same password for social media and work accounts."

Behavior: "I use a different password for my social media and work accounts."

Participants are required to respond on five-point Likert scale from 'Strongly Disagree', to 'Strongly Agree'. The total number of statements for all the focus areas is 63, and about half are negatively worded. These statements measure 21 different areas of interest. For the purpose of evaluating the impact of training methods on knowledge, attitude, and behavior, we used 36 items that are relevant to our sample and meet our aims as detailed in the following section.

C. STUDY DESIGN

To answer our research questions, four governmental agencies from diverse fields were visited Thirty-five voluntary participants were invited from each agency (140 participants in total). We initially asked participants to fill the HAIS-Q to set the baseline and record their prior knowledge and experience in the field. A between-subjects experimental design [71] was used in this study. The basic design requires four groups of 35 participants to attend different combinations of security awareness training sessions before testing their knowledge, attitude, behavior, and obtaining their feedback. First, participants were given time to read the consent form and general guidelines about the study. Then,

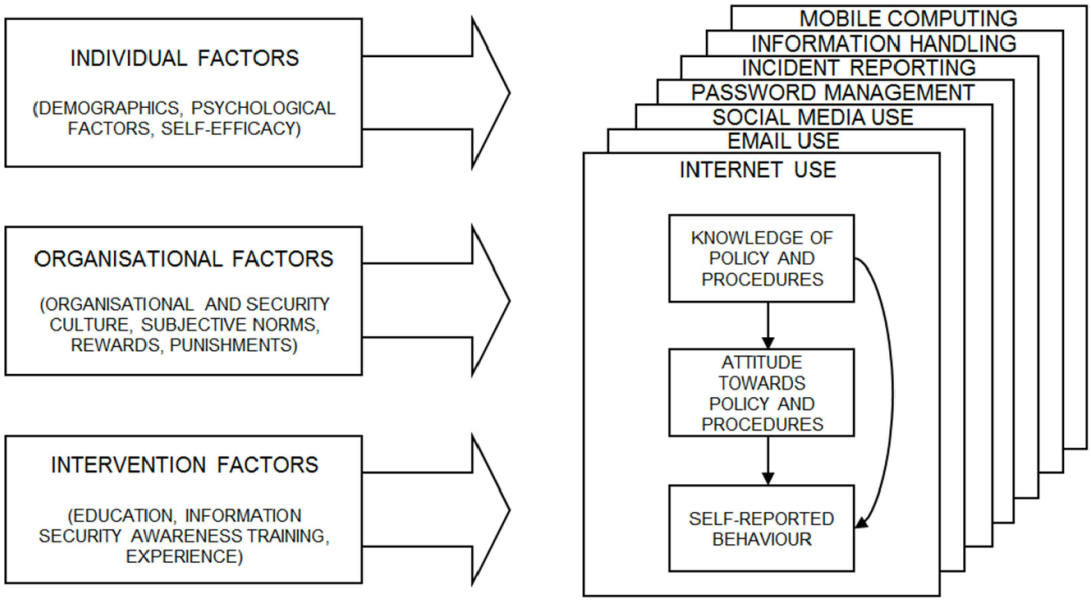

FIGURE 1. The Human Aspects of Information Security Model (adapted from [56]).

they were assigned randomly into four groups as shown in Table 2. Next, all participants attended a 30-minute lecture about general computer security topics such as password management, social engineering attacks, information handling, and physical device security. Once the lecture was complete, each group was taken to another room to continue the experiment. Group A participants watched a 30-minute video covering topics similar to those covered during the lecture. This video is a summary of multiple episodes of an information security awareness TV program that can be found at Kuwait Government Online website [43]. Group B was given reading material. Group C attended a game-based session where employees were instructed to play two web-based games for 30 minutes: Cyber Awareness Challenge [28] and Cybersecurity Lab [51]. Finally, Group D was not given any additional training. The content of all the training formats was almost identical and covered the same topics, which had also been introduced to the participants earlier in the lecture. Three weeks later, participants were invited to take part in a post-study survey in addition to the HAIS-Q to collect the required data to answer our research questions.

V. RESULTS

A. RESULTS FOR RQ1

To quantify knowledge improvement, we conducted pre- and post-tests using the HAIS questionnaire. Participants were asked to answer twelve Likert-scale type questions related to general cyber-security topics, as described in section IV-C, where 5 represents 'Strongly Disagree', and 1 means 'Strongly Agree'. Table 3 summarizes the knowledge improvement for each group. We compared knowledge scores before and after the training session for each group. On average, users performed better after the experiment than before taking the training. Wilcoxon signed rank sum tests with a confidence level of 95% ($\alpha = 0.05$) indicated that these differences were statistically significant, as detailed in Table 4 (I). We measured effect size using Cohen's d statistic [21], the effect size is considered (1) negligible if $0 < d < 0.2$, (2) small if $0.2 \leq d < 0.5$, (3) medium if $0.5 \leq d < 0.8$, or (4) large if $d \geq 0.8$. For the knowledge scores, all differences are considered large except for Group D. We used analysis of covariance (ANCOVA) to examine groups differences on post-test knowledge scores with pre-knowledge scores as a covariate. Results indicated no statistically significant difference in post-test knowledge score between the groups, $F(3, 123) = 2.028$, $p = 0.113$.

TABLE 3. Improvement results.

Group	Knowledge	Attitude	Behavior
Group A	35.20 %	31.23 %	23.12 %
Group B	38.77 %	30.33 %	26.19 %
Group C	33.62 %	32.31 %	29.10 %
Group D	27.37 %	17.52 %	15.36 %

B. RESULTS FOR RQ2

To answer this question, we followed a similar approach to the one in the previous question. In particular, we used twelve statements to obtain participants' attitudes towards a range of cyber-security statements. Participants answered the same questions in the pre- and post-study questionnaires. Attitude improvement results can be found in Table 3. A Wilcoxon signed rank sum test with a confidence level of 0.05 ($\alpha = 0.05$) shows that there is a statistically significant difference between each group's score pre- and post-training (Table 4 (II)). For attitude scores, the effect size of

TABLE 4. Results of the Wilcoxon signed rank sum test of the pre- and post-study for the four groups.

Group	p-value	Median Before - After	Standard Deviation Before - After	Cohen's d statistic	Effect Size
I- Knowledge					
Group A	< 0.01	33.0 - 44.6	11.4 - 9.17	1.087	Large
Group B	< 0.01	32.6 - 45.2	11.9 - 11.9	1.060	Large
Group C	< 0.01	32.5 - 43.5	11.5 - 12.2	0.913	Large
Group D	< 0.01	33.0 - 42.0	12.6 - 10.8	0.718	Medium
II- Attitude					
Group A	< 0.01	32.7 - 42.9	10.6 - 9.00	1.025	Large
Group B	< 0.01	32.7 - 42.6	12.4 - 11.1	0.829	Large
Group C	< 0.01	31.6 - 41.8	11.2 - 11.8	0.883	Large
Group D	< 0.01	32.8 - 38.5	11.4 - 9.83	0.501	Medium
III- Behavior					
Group A	< 0.01	30.3 - 37.3	9.89 - 8.14	0.728	Medium
Group B	< 0.01	30.8 - 38.8	11.3 - 10.4	0.732	Medium
Group C	< 0.01	29.1 - 37.6	9.57 - 9.31	0.895	Large
Group D	< 0.01	29.8 - 34.4	10.9 - 10.0	0.433	Small

Group A, B, and C was large, compared to medium for Group D. To further investigate the impact of each training method on employees' attitudes after controlling for pre-test scores, we ran an ANCOVA test. There was a statistically significant difference in attitude score between the groups, $F(3, 123) = 3.861$, $p = 0.011$. Post-hoc analysis was performed using a Bonferroni correction. The mean post-test attitude score was statistically higher in Group A than in Group D ($t(123) = 2.93$, $p = 0.024$). Results also showed that Group B ($t(123) = 2.70$, $p = 0.047$) and Group C ($t(123) = 2.73$, $p = 0.043$) scores are significantly better than the Group D score.

C. RESULTS FOR RQ3

For this question, participants rated twelve statements with regard to a number of general situations related to computer and information security. Table 3 show the results of behavioral improvement for the groups. Although all groups' training methods improved users' behavior significantly (Table 4-III), a difference in the amount of change and effect size between the groups was evident. An ANCOVA with a Bonferroni post-hoc test revealed that post-test attitude scores differed across groups $F(3, 123) = 4.000$, $p = 0.009$. Specifically, a significant difference was found between Group B when compared to Group D, $t(123) = 2.99$, $p = 0.0033$. Similarly, Group C reported significantly higher scores than Group D, $t(123) = 3.02$, $p = 0.003$.

D. RESULTS FOR RQ4

We asked those who completed the entire experiment to rate four statements from 1 (Lowest) to 10 (Highest) regarding their training experience:

Q1- Overall, how do you rate the training program?

Q2- Do you feel that you now have a better understanding of cyber-threats?

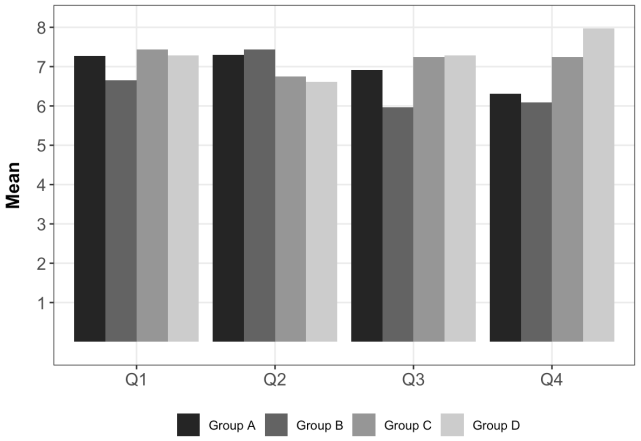

FIGURE 2. Mean scores for satisfaction questions.

Q3- How likely is it that you will voluntarily participate in future cyber-security awareness training programs?

Q4- How do you rate the length of the training program?

Figure 2 summarizes the results. For the first question, there were differences in the programs ratings across the groups: Group A ($M = 7.27$, $SD = 1.40$), Group B ($M = 6.65$,, $SD = 2.25$), Group C ($M = 7.43$, $SD = 1.46$), and Group D ($M = 7.29$,, $SD = 1.79$). However, a one-way ANOVA analysis indicated that these differences were insignificant $F(3, 124) = 1.247$, $p = 0.296$.

For the second question (Q2), employees felt that having a lecture combined with reading session (Group B, $M = 7.43$, $SD = 1.27$) or watching a video (Group A, $M = 7.3$, $SD = 1.40$) made them feel better about their understanding of the topic than playing a game (Group C, $M = 6.75$, $SD = 1.74$) and/or lecture only session (Group D $M = 6.61$, $SD = 2.06$). Inspecting these differences using one-way ANOVA shows that no statistically significant difference exists between the four groups $F(3, 124) = 1.939$, $p = 0.127$.

For Q3, participants showed more interest in future training campaigns similar to (Group D, M = 7.26, SD = 2.00) and (Group C, M = 7.22, SD = 2.11), followed by (Group A, M = 6.91, SD = 1.89) and (Group B, M = 6.0, SD = 1.81). An ANOVA analysis indicated a statistically significant difference among the groups $F(3, 124) = 3.215$, $p = 0.025$. In fact, a Tukey (HSD) post-hoc test showed that participants from the self-reading session (Group B) scored significantly lower than game-based session (Group C, $p = 0.044$) and lecture-only session (Group D, $p = 0.037$). However, no statistically significant difference was found between Group A and B ($p = 0.209$).

Finally, for Q4, respondents indicated that the length of the training program was reasonable for Group D (M = 7.97, SD = 1.20) and Group C (M = 7.25, SD = 2.08), compared to Group A (M = 6.30, SD = 1.53) and Group B (M = 6.09, SD = 1.65). A one-way ANOVA analysis indicated that these differences were significant $F(3, 124) = 8.817$, $p < 0.001$. Analysing the results of a Tukey (HSD) post-hoc test shows that Group D results are considerably higher than Group A ($p = 0.0005$) and Group B ($p<0.0001$). Also, Group C scored significantly higher than Group B ($p = 0.029$).

To investigate the correlation between the four questions, we ran a series of Pearson correlation coefficients. Not surprisingly, a large significant positive correlation was found between the program's rating (Q1) and user's willingness to participate in future training programs (Q3) ($r = 0.622$, $p < 0.001$). Furthermore, there was a positive correlation between the overall rating (Q1) and the perceived length of the program (Q4) ($r = 0.517$, $p < 0.001$). Additionally, there was a correlation between Q3 and Q4 ($r = 0.847$, $p < 0.001$). For the other questions, however, no significant correlation was observed.

VI. THREATS TO VALIDITY

A. INTERNAL VALIDITY

Internal validity threats are those that might influence the confidence we have in the cause-and-effect relationship. The first limitation is the fact that all participants are volunteers and there is no direct consequence of their answers. According to [60], subjects change their behavior observations under laboratory conditions, and they may respond differently if there is an opportunity cost or a negative outcome to their selections. Moreover, the validity of self-report behavior has been criticized in the literature [60], [69], as participants may tend to hide their irresponsible risky activities due to social desirability bias. Therefore, we implemented a few of the measures proposed in [29]. For instance, we assured the participants' anonymity and confidentiality. Additionally, we did not ask them for their name or any other personal information that might identify them. Although there is no guarantee that these measures were enough to be certain that all respondents were reporting their actual behavior, a study by [84] found a correlation between what the participants reported and what they actually did regarding phishing emails. Moreover, researchers [19], [70] argued that self-report studies are considered an important tool for hypotheses testing especially for empirical research. Finally, all objective measures of cybersecurity behavior have their own limitations [41], since incidents often go unreported or undetected [37], [56]. Thus, self-report is considered suitable for this work.

Survivorship bias is another concern in our study, so we only included the results for those who completed the experiment to the end. The Hawthorne effect [64] may have affected the results of Group D. However, we tried to minimize this effect by separating the groups into four different rooms immediately after taking the lecture. Finally, to reduce recall and carryover effects [7], we waited a sufficient period between the two tests.

B. EXTERNAL VALIDITY

Our ability to generalize the findings is within the domain of this threat. Our results are based on employees-in-practice from various organizations and fields. The participants are from various age cohorts, educational backgrounds, and ethnic groups. However, it cannot be claimed that our results can be generalized for all people or organizations. Further empirical research is required across a wider variety of settings to confirm our findings and improve the chance of generalizability. Another area of concern is the effect of teacher assignments. According to [74], participants performance can be influenced considerably by the instructors. Therefore, we minimized this effect by gathering all subjects in a conference room to attend the lecture before assignment in their groups. Additionally, our results are based on the cyber-security topics we covered in our study; more research is needed to validate these results with a broader topics and domains.

C. CONSTRUCT VALIDITY

Construct validity refers to the relationship between the theoretical constructs and what we observed. In our study, most of our results were measured using the Human Aspects of Information Security Questionnaire (HAIS-Q) which has been used and validated in a large number of studies and widely accepted as a good measurement tool for ISA programs [55]. HAIS-Q is based on the Knowledge-Attitude-Behavior (KAB) model that is adopted as a standard by many experts. Moreover, the materials we used to compare the groups in our study were used and validated in previous peer-reviewed published research. A possible construct threat is the lack of similar studies that used the same approach; thus, we are not able compare our results with other works. We plan, however, to expand this study in the future to include general internet users in order to compare the results.

D. CONCLUSION VALIDITY

This threat is concerned with the degree to which the findings and conclusions we draw from statistical analysis of the data are appropriate and accurate. To test the existence of a significant difference after the treatments, we used the Wilcoxon signed rank sum test with a confidence level of

95% ($\alpha = 0.05$), since it does not require the data to be normally distributed. To compare the groups, we used Analysis of covariance (ANCOVA) to correct for preexisting differences between groups. Six assumptions underlying the use of ANCOVA were tested before using it to analyze the data. Similarly, prior to proceeding with ANOVA analysis of satisfaction results, we confirmed that none of the assumptions were violated. We may therefore be assured that the statistical relationships we have found are significant.

VII. DISCUSSIONS

In this section we discuss the implications of our results. To begin with knowledge findings, we see that all the training methods increased participants' knowledge about the topic between 27.37% (Group D) and 38.77% (Group B). The improvement in knowledge is expected after a training session. First, about 40% of the participants were juniors who may not have received enough training since joining the organization. Furthermore, the topic that we need to convey is complex and continuously evolving, thus employee's knowledge and skills need to be updated periodically. Moreover, the post-study was performed three weeks after the experiment, so the information was fresh in the subjects' minds while taking the questionnaire. *Therefore, when the main objective of a training campaign is to raise awareness regarding security threats, it does not matter which format is chosen.* In practice, however, more often than not ISA training is performed to increase employee's compliance with security guidelines and policies in order to secure organizations against internal and external threats.

According to the 'Security, Functionality and Usability Triangle' theory [79], strict security measures reduce the usability and the functionality of a system. Hence, to ask employees to voluntarily give away some of the freedom they have in using the systems, a mindset change is needed. The findings of the second research question illustrate that knowledge transfer in all formats was somehow successful in changing respondents' attitudes, but there was a considerable gap between those who received the message using multiple formats and those who attended one session. *In other words, delivering the same message in multiple ways was more effective in changing employees' attitudes towards the importance of security measures than delivering it only once.*

According to the KAB model, knowledge and attitude are vehicles for behavioral change. Despite the improvement in behavioral scores for all groups, text-based and game-based groups stood out. Here, we see that giving a lecture only (Group D) or instructor-led training complemented by multimedia (Group A) may have improved user's knowledge, but that did not reflect in the employees' actions as strongly as that in the text-based and game-based sessions. It is worth mentioning that for Group D, participants received training for a shorter period (30 minutes) since they did not attend a follow-up session, as all other three groups did. However, in Group A (video), despite having the message in two formats, the employees' attitudes did not differ significantly than those who had only one treatment. This might be due the fact that in both lectures and video training, participants may choose to remain passive while listening to the instructor or watch the video without engagement from subjects. In addition, educating employees and raising their knowledge "does not reflect the idea of prescriptiveness" [67]. In other words, employees may know the security policies and guidelines, but they may deliberately choose to not comply with them. To further investigate the 8-point gap between attitude and behavior scores for Group A, we had a closer look at participants' qualitative responses. A considerable number of respondents indicated that they truly believe in the importance of many security measures, but they did not have the time to change their passwords or review privacy settings. Put another way, video session participants were not convinced of the urgency of the security guidelines, despite agreeing with its importance. It is noteworthy that Group C was the most consistent group in terms of improvement across the three constructs. In contrast, all the other three groups dropped more than 10 percentage points between their knowledge and attitude scores. This may be due the fact that games provide a simulation of real practical scenarios where employees can see the consequences of their actions immediately. Moreover, in some games participants are not able to proceed to the next level without choosing the correct decision. *In short, text-based and game-based participants significantly outperformed other employees in behavioral change.*

The final research question intended to obtain employees feedback about their training method preferences. Overall, the respondents who took part in the self-reading session reported that their understanding of the cyber-threats had increased more than all other groups, yet their training experience obtained the lowest rating. Although the groups did not differ significantly in this regard, we see that overwhelming employees with too much technical information can cause a negative effect. This was evident in the participants' response when they were asked about their enthusiasm towards participating in future ISA training programs (Q3) and their opinion about the length of the program (Q4). The aforementioned result emphasizes on the importance of making the training engaging and interesting [6], [85], which has multiple implications. First, when the program is interesting, trainees are more likely to stay committed to completing the entire training program. Second, it raises the chance of employees taking the initiative to effectively participate in future training programs and drives employees toward more self-development activities [5], [34], [61]. Third, engagement could increase among trainees and spread knowledge faster through peer-to-peer interaction [17], [45], [46]. Additionally, according to the National Institute of Standards in Technology report [54], minimizing "security fatigue" is crucial to keep employees focused on what is important. Many recent security breach incidents were due to the large amount of false warnings which make employees and even IT professionals treat them as a norm [38].

VIII. CONCLUSION AND FUTURE WORK

Cyber-security awareness is vital in reducing security breaches, especially those caused by employees' naive and accidental behaviors. There are multiple ways in which organizations can educate their employees. In this paper, we compared the impact of different intervention strategies on employees' knowledge, attitudes, and behaviors towards security measures. We used HAIS-Q, which is based on the KAB model, as an instrument for measuring employees' awareness. *Results indicated that all the methods are comparable in knowledge improvement; however, there was a significant gap in employees' attitude, behavior, and satisfaction scores between the groups. In particular, employees who attended two different training methods performed better in terms of attitude improvement than those who attended a lecture only. Additionally, text-based and game-based participants significantly outperformed other employees in behavioral change. Finally, results showed a correlation between training program enjoyment and perceived training session's length. Furthermore, users' attitude toward their participation in future awareness campaigns is highly influenced by their overall training experience.* These results have several implications, for instance, security stress and fatigue can be reduced by choosing the appropriate training strategy. This, as a result, reduces employees' feeling of being overwhelmed and forced to follow guidelines in addition to staying vigilant for all the alerts and warnings they may face daily. Moreover, employees will more likely stay committed during the entire program and will engage more with other trainees leading to an improved peer-to-peer knowledge-sharing. Finally, it will improve the chances of self-development initiatives leading to more secure organizations.

Although the paper examines and compares different ISA methods and has identified each one's effectiveness, this work has several limitations which give rise to a number of future research lines. One of the limitations is that this study is based on a self-report instrument, whilst other researchers have already used and tested the framework in various organizational settings (section VI), we plan to validate our respondents' answers with their actual behavior by analyzing their system logs before and after the training. Another dimension to explore is to further investigate the impact of individual factors on user perception of the training program. In particular, we plan to study the relation among sociodemographic factors and user performance. Additionally, we intend to study in the future the long-term impact of different intervention strategies on knowledge, attitude, and behavior. Finally, an open issue for future research is to study the impact of personalizing training programs to match individual's learning style preference and personality profiles.

A. RESEARCH CONTRIBUTIONS

This research has made several contributions to research and practice. The study offers two main contributions to the wider information system security field. It addresses the lack of cross-cultural Information Security research by collecting data from Kuwaiti organizations. [25] argued that a major limitation of Information Security research was that it tended to be conducted in Western cultures without data from the rest of the world. Therefore, a study performed in relation to a Middle Eastern culture (Kuwait) helps raise awareness to both researchers and practitioners about ISA methods in a way conducive to influencing employees' knowledge, attitude, or behavior. Additionally, the study employs interventions and field experiments to address a shortcoming of survey-based research reported in [25]. Relatedly, while most studies in the field use student subjects to collect the data due to the difficulties faced in accessing organizations, this study was conducted with employees; therefore, the findings are more relevant to organizational settings. Another key difference is that the study empirically tested the impact of the different training strategies on users' knowledge, attitude, and behavior, taking a holistic approach to the different aspects of ISA using HAIS-Q rather than focusing on one (e.g., email management or phishing).

The study has several implications for practice. First, the findings enable organizations to better utilize their resources by selecting the ISA methods that fit their objectives. Companies consequently find their preferred trade-offs between the desired security degree and the amount of resources needed to accomplish it. For instance, if the goal of the organization were to simply raise awareness, they could chiefly consider factors such as cost, time-efficiency, or user preference instead of focusing heavily in the program's format since all intervention strategies lead to similar results. This not only conserves time and resources but also reduces the pressure on the employees, allowing them to maintain focus on their primary work activities. Conversely, if the objective were to change employees' security habits, then the ISA method should be modified carefully to achieve that goal. Although a combination of ISA formats was more effective in increasing awareness about the topics, using the wrong delivery format could negatively impact an employee's rating of the program, and they might view it as "just another obligatory session," [82] creating a false sense of security and potentially causing security fatigue. Therefore, engaging and interesting ISA programs are especially important in motivating employees to voluntarily participate in future self-education activities and in diffusing the messages faster across an organization through peer-to-peer knowledge sharing.

REFERENCES

[1] J. Abawajy, "User preference of cyber security awareness delivery methods," *Behav. Inf. Technol.*, vol. 33, no. 3, pp. 237–248, Mar. 2014.

[2] N. H. A. Rahim, S. Hamid, M. L. M. Kiah, S. Shamshirband, and S. Furnell, "A systematic review of approaches to assessing cybersecurity awareness," *Kybernetes*, vol. 44, no. 4, pp. 606–622, Apr. 2015.

[3] A. Acquisti and R. Gross, "Imagined communities: Awareness, information sharing, and privacy on the Facebook," in *Proc. Int. Workshop Privacy Enhancing Technol.* Cham, Switzerland: Springer, 2006, pp. 36–58.

[4] A. Ahmad, K. C. Desouza, S. B. Maynard, H. Naseer, and R. L. Baskerville, "How integration of cyber security management and incident response enables organizational learning," *J. Assoc. Inf. Sci. Technol.*, vol. 71, no. 8, pp. 939–953, Aug. 2020.

[5] M. Ainley and J. Ainley, "Student engagement with science in early adolescence: The contribution of enjoyment to students' continuing interest in learning about science," *Contemp. Educ. Psychol.*, vol. 36, no. 1, pp. 4–12, Jan. 2011.
[6] E. Albrechtsen and J. Hovden, "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study," *Comput. Secur.*, vol. 29, no. 4, pp. 432–445, Jun. 2010.
[7] M. J. Allen and W. M. Yen, *Introduction to Measurement Theory*. Long Grove, IL, USA: Waveland Press, 2001.
[8] M. Alshaikh, "Developing cybersecurity culture to influence employee behavior: A practice perspective," *Comput. Secur.*, vol. 98, Nov. 2020, Art. no. 102003.
[9] M. Alshaikh, A. Ahmad, S. B. Maynard, and S. Chang, "Towards a taxonomy of information security management practices in organisations," in *Proc. 25th Australas. Conf. Inf. Syst.*, Auckland, New Zealand, Dec. 2014.
[10] M. Alshaikh, S. B. Maynard, and A. Ahmad, "Security education, training, and awareness: Incorporating a social marketing approach for behavioural change," in *Proc. Int. Inf. Secur. Conf.* Cham, Switzerland: Springer, 2020, pp. 81–95.
[11] M. Alshaikh, S. B. Maynard, and A. Ahmad, "Applying social marketing to evaluate current security education training and awareness programs in organisations," *Comput. Secur.*, vol. 100, Jan. 2021, Art. no. 102090.
[12] M. Alshaikh, S. B. Maynard, A. Ahmad, and S. Chang, "An exploratory study of current information security training and awareness practices in organizations," in *Proc. 51st Hawaii Int. Conf. Syst. Sci.*, 2018, pp. 5085–5094.
[13] M. Alshaikh, H. Naseer, A. Ahmad, and S. B. Maynard, "Toward sustainable behaviour change: An approach for cyber security education training and awareness," in *Proc. 27th Eur. Conf. Inf. Syst. (ECIS)*, Stockholm, Sweden, 2019, pp. 1–14.
[14] N. A. G. Arachchilage and S. Love, "Security awareness of computer users: A phishing threat avoidance perspective," *Comput. Hum. Behav.*, vol. 38, pp. 304–312, Sep. 2014.
[15] G. Assenza, A. Chittaro, M. C. De Maggio, M. Mastrapasqua, and R. Setola, "A review of methods for evaluating security awareness initiatives," *Eur. J. Secur. Res.*, vol. 5, pp. 1–29, Oct. 2019.
[16] M. Bada, A. M. Sasse, and J. R. C. Nurse, "Cyber security awareness campaigns: Why do they fail to change behaviour?" 2019, *arXiv:1901.02672*.
[17] J. P. Bean, "Dropouts and turnover: The synthesis and test of a causal model of Student attrition," *Res. Higher Educ.*, vol. 12, no. 2, pp. 155–187, 1980.
[18] T. Caldwell, "Making security awareness training work," *Comput. Fraud Secur.*, vol. 2016, no. 6, pp. 8–14, Jun. 2016.
[19] D. Chan, "So why ask me? Are self-report data really that bad?" in *Statistical and Methodological Myths and Urban Legends*. Evanston, IL, USA: Routledge, 2009, pp. 309–336.
[20] N. Clarke, J. Symes, H. Saevanee, and S. Furnell, "Awareness of mobile device security: A survey of user's attitudes," *Int. J. Mobile Comput. Multimedia Commun.*, vol. 7, no. 1, pp. 15–31, Jan. 2016.
[21] J. Cohen, *Statistical Power Analysis for the Behavioral Sciences*. New York, NY, USA: Academic, 2013.
[22] P. Coopers. (2018). *Global State of Information Security Survey 2018*. Accessed: Nov. 3, 2021. [Online]. Available: https://www.pwc.com/sg/en/publications/assets/gsiss-2018.pdf
[23] A. Corallo, M. Lazoi, M. Lezzi, and A. Luperto, "Cybersecurity awareness in the context of the industrial Internet of Things: A systematic literature review," *Comput. Ind.*, vol. 137, May 2022, Art. no. 103614.
[24] *Best Practices for Implementing a Security Awareness Program*, PCI Secur. Standards Council, Wakefield, MA, USA, 2014.
[25] R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville, "Future directions for behavioral information security research," *Comput. Secur.*, vol. 32, pp. 90–101, Feb. 2013.
[26] M. C. De Maggio, M. Mastrapasqua, M. Tesei, A. Chittaro, and R. Setola, "How to improve the security awareness in complex organizations," *Eur. J. Secur. Res.*, vol. 4, no. 1, pp. 33–49, Apr. 2019.
[27] Deloitte. (2020). *Deloitte Cyber Survey*. Accessed: Nov. 3, 2021. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/dk/Documents/Cyber/cyberreport/Cyber_survey_.pdf
[28] DoD. (2020). *Cyber Awareness Challenge*. [Online]. Available: https://public.cyber.mil/training/cyber-awareness-challenge/
[29] S. I. Donaldson and E. J. Grant-Vallone, "Understanding self-report bias in organizational behavior research," *J. Bus. Psychol.*, vol. 17, no. 2, pp. 245–260, 2002.
[30] T. Fertig, A. E. Schütz, and K. Weber, "Current issues of metrics for information security awareness," in *Proc. ECIS*, 2020.
[31] FireEye. (2020). *M-Trends Reports*. [Online]. Available: https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html
[32] C. C. Fung, V. Khera, A. Depickere, P. Tantatsanawong, and P. Boonbrahm, "Raising information security awareness in digital ecosystem with games—A pilot study in Thailand," in *Proc. 2nd IEEE Int. Conf. Digit. Ecosystems Technol.*, Feb. 2008, pp. 375–380.
[33] P. Fung and D. Longley, "Electronic information security documentation," in *Proc. Australas. Inf. Secur. Workshop Conf. ACSW Frontiers*, vol. 21, 2003, pp. 25–31.
[34] J. P. Gee, "What video games have to teach us about learning and literacy," *Comput. Entertainment*, vol. 1, no. 1, p. 20, Oct. 2003.
[35] S. Goodman, D. W. Straub, and R. Baskerville, *Information Security: Policy, Processes, and Practices*. Evanston, IL, USA: Routledge, 2016.
[36] A. Guillot and S. Kennedy, "Information security surveys: A review of the methodologies, the critics and a pragmatic approach to their purposes and usage," in *Proc. Austral. Inf. Secur. Manage. Conf.*, 2007, p. 25.
[37] L. Hadlington and K. Parsons, "Can cyberloafing and internet addiction affect organizational information security?" *Cyberpsychol., Behav., Social Netw.*, vol. 20, no. 9, pp. 567–571, Sep. 2017.
[38] W. He and Z. Zhang, "Enterprise cybersecurity training and awareness programs: Recommendations for success," *J. Organizational Comput. Electron. Commerce*, vol. 29, no. 4, pp. 249–257, Oct. 2019.
[39] T. Herath and H. R. Rao, "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decision Support Syst.*, vol. 47, no. 2, pp. 154–165, 2009.
[40] *Information Technology—Security Techniques—Code of Practice for Information Security Controls*, document ISO/IEC27002, 2013.
[41] M. Kabay. (2001). *Studies and Surveys of Computer Crime*. [Online]. Available: http://www2.norwich.edu/mkabay/methodology/crime_studies.html
[42] Kaspersky. (2020). *The Human Factor in it Security*. [Online]. Available: https://www.kaspersky.com/blog/the-human-factor-in-it-security
[43] KGO. (2020). *Awareness Section*. [Online]. Available: https://www.e.gov.kw/sites/kgoEnglish/Pages/Citizens-Residents/Awareness/BaytakPage.aspx
[44] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Comput. Secur.*, vol. 25, no. 4, pp. 289–296, Jun. 2006.
[45] O. T. Lenning and L. H. Ebbers, "The powerful potential of learning communities: Improving education for the future," in *ASHE-ERIC Higher Education Report*, vol. 26, no. 6. London, U.K.: ERIC, 1999.
[46] Y. Li, E. McCoy, M. C. Shelley, and D. F. Whalen, "Contributors to student satisfaction with special program (fresh start) residence Halls," *J. College Student Develop.*, vol. 46, no. 2, pp. 176–192, 2005.
[47] A. McCormac, D. Calic, K. Parsons, M. Butavicius, M. Pattinson, and M. Lillie, "The effect of resilience and job stress on information security awareness," *Inf. Comput. Secur.*, vol. 26, no. 3, pp. 277–289, Jul. 2018.
[48] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius, and M. Pattinson, "Individual differences and information security awareness," *Comput. Hum. Behav.*, vol. 69, pp. 151–156, Apr. 2017.
[49] C. Murchison, *A Handbook of Social Psychology*. Worcester, MA, USA: Clark Univ. Press, 1935, pp. 789–844.
[50] A. Mylonas, A. Kastania, and D. Gritzalis, "Delegate the smartphone user? Security awareness in smartphone platforms," *Comput. Secur.*, vol. 34, pp. 47–66, May 2013.
[51] NOVALabs. (2020). *Cybersecurity Lab*. [Online]. Available: https://www.pbs.org/wgbh/nova/labs/lab/cyber/
[52] G. Ögütçü, Ö. M. Testik, and O. Chouseinoglou, "Analysis of personal information security behavior and awareness," *Comput. Secur.*, vol. 56, pp. 83–93, Feb. 2016.
[53] T. Olovsson, "A structured approach to computer security," Chalmers Univ. Technol., Gothenburg, Sweden, Tech. Rep. 122, 1992.
[54] P. D. O'Reilly, K. G. Rigopoulos, G. A. Witte, and L. Feldman, "2017 NIST/ITL cybersecurity program: Annual report," NIST Special Publications, Gaithersburg, MD, USA, Tech. Rep. NIST SPECIAL PUBLICATION 800-206, 2018, doi: 10.6028/NIST.SP.800-206.
[55] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The human aspects of information security questionnaire (HAIS-Q): Two further validation studies," *Comput. Secur.*, vol. 66, pp. 40–51, May 2017.

[56] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q)," *Comput. Secur.*, vol. 42, pp. 165–176, May 2014.
[57] K. Parsons, A. McCormac, M. Pattinson, M. Butavicius, and C. Jerram, "A study of information security awareness in Australian government organisations," *Inf. Manage. Comput. Secur.*, vol. 22, no. 4, pp. 334–345, Oct. 2014.
[58] M. Pattinson, M. Butavicius, M. Lillie, B. Ciccarello, K. Parsons, D. Calic, and A. McCormac, "Matching training to individual learning styles improves information security awareness," *Inf. Comput. Secur.*, vol. 28, no. 1, pp. 1–14, Nov. 2019.
[59] G. Piccoli and F. Pigni, *Information Systems for Managers: With Cases*. Burlington, VT, USA: Prospect Press, 2019.
[60] P. M. Podsakoff and D. W. Organ, "Self-reports in organizational research: Problems and prospects," *J. Manage.*, vol. 12, no. 4, pp. 531–544, 1986.
[61] C. N. Quinn, *Engaging Learning: Designing E-Learning Simulation Games*. Hoboken, NJ, USA: Wiley, 2005.
[62] R. M. Ryan and E. L. Deci, "Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being," *Amer. Psychol.*, vol. 55, no. 1, p. 68, 2000.
[63] N. S. Safa, R. Von Solms, and S. Furnell, "Information security policy compliance model in organizations," *Comput. Secur.*, vol. 56, pp. 70–82, Feb. 2016.
[64] D. W. Schanzenbach, "Limitations of experiments in education research," *Educ. Finance Policy*, vol. 7, no. 2, pp. 219–232, Apr. 2012.
[65] R. S. Shaw, C. C. Chen, A. L. Harris, and H.-J. Huang, "The impact of information richness on information security awareness training effectiveness," *Comput. Educ.*, vol. 52, no. 1, pp. 92–100, Jan. 2009.
[66] M. Siponen and R. Willison, "Information security management standards: Problems and solutions," *Inf. Manage.*, vol. 46, no. 5, pp. 267–270, Jun. 2009.
[67] M. T. Siponen, "A conceptual foundation for organizational information security awareness," *Inf. Manage. Comput. Secur.*, vol. 8, no. 1, pp. 31–41, Mar. 2000.
[68] A. Solomon, M. Michaelshvili, R. Bitton, B. Shapira, L. Rokach, R. Puzis, and A. Shabtai, "Contextual security awareness: A context-based approach for assessing the security awareness of users," *Knowl.-Based Syst.*, vol. 246, Jun. 2022, Art. no. 108709.
[69] P. E. Spector, "A consideration of the validity and meaning of self-report measures of job conditions," *Int. Rev. Ind. Organizational Psychol.*, vol. 1992, pp. 123–151, Jun. 1992.
[70] P. E. Spector, "Using self-report questionnaires in OB research: A comment on the use of a controversial method," *J. Organizational Behav.*, vol. 15, no. 5, pp. 385–392, Sep. 1994.
[71] C. Stangor, *Research Methods for the Behavioral Sciences*. Toronto, ON, Canada: Nelson Education, 2014.
[72] S. Stockhardt, B. Reinheimer, M. Volkamer, P. Mayer, A. Kunz, P. Rack, and D. Lehmann, "Teaching phishing-security: Which way is best?" in *Proc. IFIP Int. Conf. ICT Syst. Secur. Privacy Protection*. Cham, Switzerland: Springer, 2016, pp. 135–149.
[73] Symantec. (2019). *What is Social Engineering? Tips to Help Avoid Becoming a Victim*. [Online]. Available: https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html
[74] K. Topping, "Self and peer assessment in school and university: Reliability, validity and utility," in *Optimising New Modes Assessment: In Search Qualities Standards*. Cham, Switzerland: Springer, 2003, pp. 55–87.
[75] K. F. Tschakert and S. Ngamsuriyaroj, "Effectiveness of and user preferences for security awareness training methodologies," *Heliyon*, vol. 5, no. 6, Jun. 2019, Art. no. e02010.
[76] S. Utz and N. C. Krämer, "The privacy paradox on social network sites revisited: The role of individual characteristics and group norms," *Cyberpsychol., J. Psychosocial Res. Cyberspace*, vol. 3, no. 2, 2009.
[77] Verizon. (2020). *Data Breach Investigations Report*. [Online]. Available: https://enterprise.verizon.com/resources/reports/dbir/
[78] C. Vroom and R. von Solms, "Towards information security behavioural compliance," *Comput. Secur.*, vol. 23, no. 3, pp. 191–198, May 2004.
[79] A. Waite. (2010). *Infosec Triads: Security/Functionality/Ease-of-Use*. [Online]. Available: https://blog.infosanity.co.uk/?p=676
[80] M. E. Whitman and H. J. Mattord, *Principles of Information Security*. Boston, MA, USA: Cengage Learning, 2011.
[81] A. Wiley, A. McCormac, and D. Calic, "More than the individual: Examining the relationship between culture and information security awareness," *Comput. Secur.*, vol. 88, Jan. 2020, Art. no. 101640.
[82] M. Wilson and J. Hash, "Building an information technology security awareness and training program," *NIST Special Publication*, vol. 800, no. 50, pp. 1–39, 2003.
[83] M. Wolf, D. Haworth, and L. Pietron, "Measuring an information security awareness program," *Rev. Bus. Inf. Syst.*, vol. 15, no. 3, pp. 9–22, Jul. 2011.
[84] M. Workman, "Gaining access with social engineering: An empirical study of the threat," *Inf. Syst. Secur.*, vol. 16, no. 6, pp. 315–331, Dec. 2007.
[85] C. Yi-Cheng, L. Yi-Chien, R. C. Yeh, and L. Shi-Jer, "Examining factors affecting college students' intention to use web-based instruction systems: Towards an integrated model," *Turkish Online J. Educ. Technol.*, vol. 12, no. 2, pp. 111–121, 2013.
[86] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber security awareness, knowledge and behavior: A comparative study," *J. Comput. Inf. Syst.*, vol. 62, no. 1, pp. 82–97, Jan. 2022.

BADER ALKHAZI received the Ph.D. degree in information systems engineering from the University of Michigan, in 2019. Before pursuing his Ph.D., he worked for four years at the Central Agency for Information Technology: a governmental institute that supervises the implementation of national IT plans and e-government projects of immense scope in Kuwait. He is currently an Assistant Professor of information science at Kuwait University. His current research interests include cybersecurity, blockchain, educational technologies, software engineering, and e-government.

MONEER ALSHAIKH received the master's degree in information technology with specialization in networking and security and the Ph.D. degree in information security management. He worked as a Research Fellow in cybersecurity at the Academic Centre of Cyber Security Excellence, University of Melbourne. He is currently an Associate Professor at the College of Computer Science and Engineering, University of Jeddah. He is also a cybersecurity professional with outstanding knowledge and experience gained through years of research, teaching, and mentoring. He received certificates in management and leadership, and teaching in higher education and ISO 27001 implementation.

SULAIMAN ALKHEZI received the bachelor's degree in computer science from Kuwait University, in 2005, and the master's degree from Kent State University, in 2010. He is currently a Research Assistant at Kuwait University. His current research interests include e-learning, information security, and psycholinguistics.

HAMZA LABBACI received the Ph.D. degree in computer science from the University of Science and Technology, Algeria. He spent one year at the University of Michigan working with Prof. Brahim Medjahed on various projects concerning machine learning and big data techniques. He is currently a Research and Teaching Assistant at the University of Tours, France.