IJRRS
International Journal of Reliability, Risk and Safety: Theory and Application

Online ISSN: 2676-3346

OPEN ACCESS

Vol. 6/ Issue 2/ 2023/ pp. 47-53
DOI: 10.22034/IJRRS.2023.6.2.6
Received: 16 August 2023, Revised: 30 September 2023, Accepted: 22 October 2023
Available online at: https://www.ijrrs.com

Original Research Article

Analysis of “Evaluation of Cybersecurity Culture and Awareness Scale (ECSCAS)” based on Polychotomous models of Item Response Theory (IRT)

Sedigheh Heydari[1]*

1- Department of Psychology, Human Science Faculty, Islamic Azad University, Saveh Branch, Iran

*** heydari_ss@yahoo.com**

Abstract

Recently, many private companies and government organizations worldwide have been facing the problem of cyber-attacks and the risk of wireless communication technologies. Today's world is highly dependent on electronic technology, and protecting this data against cyber-attacks is challenging. The goal of cyber-attacks is to harm companies financially, and in some cases, these attacks can have military or political goals. Therefore, the present research was conducted quantitatively to analyze the evaluation of cybersecurity culture and awareness scale in 2022 among the employees of the country bank. The statistical sample was 841 employees of bank branches. The research instrument was the "Evaluation of Cybersecurity Culture and Awareness" scale (2022), and the GRM model (common model in IRT for polychotomous data analysis) was used to analyze the data. The findings showed that all 34 items in this scale have a discriminative index, awareness index, and appropriate ability level in the target sample. Also, the highest level of awareness was between +1 and +2, and the maximum total awareness was equal to 70, which showed the desirability of the entire scale level. Examining the status of bank employees in relation to the culture and awareness of cybersecurity also showed that the status of bank employees is suitable in all 6 effective factors in promoting the culture and awareness of cybersecurity. Therefore, by using this tool, it is possible to measure the level of cybersecurity culture and awareness. In line with that, the necessary training and strategies can be carried out to improve and upgrade the existing situation in public and private organizations.

Keywords: Evaluation; Cybersecurity; Culture and Awareness; Polychotomous models; Item-response theory.

1. Introduction

Recently, many private companies and government organizations worldwide have been facing the problem of cyberattacks and the risk of wireless communication technologies. Today's world is highly dependent on electronic technology, and protecting this data from cyberattacks is challenging. The purpose of cyberattacks is to harm companies financially. In some other cases, cyberattacks can have military or political objectives. These damages include PC viruses, data distribution services, and other attack vectors. For this purpose, different organizations use different solutions to prevent damage caused by cyberattacks. Cyber security follows real-time information about the latest IT data, and so far, researchers worldwide have proposed various methods to prevent cyber-attacks or reduce the damage caused by them; some of these methods are in the operational phase, and others are in the study stage [1].

In addition, the revolution in the Information Technology (IT) field has led to a significant increase in the number of people connected to and utilizing the Internet. However, it has also introduced severe security risks: valuable information such as passwords, financial accounts, and other confidential data are considered attractive targets for attackers. Cyber-attacks against this infrastructure can not only lead to data leakage but can also have significant financial implications and even lead to loss of life. Consequently, to defend against such attacks, and considering that humans have a key role in these technologies, it is important to increase cyber-security awareness [2] because the unawareness of users about threats that can be faced in cyberspace can cause the successful execution of such threats [3].

The impact of cyberspace can be evaluated from different aspects, such as the concept of security, the disappearance of the geographical dimension of cyber threats, and the degree of vulnerability caused by cyber

How to cite this article:
S. Heydari. “Analysis of “Evaluation of Cybersecurity Culture and Awareness Scale (ECSCAS)” based on Polychotomous models of Item Response Theory (IRT)" based on Polychotomous models of Item Response Theory (IRT),” *International Journal of Reliability, Risk and Safety: Theory and Application*, vol. 6, no. 2, pp. 47-53, 2023.

threats. National security can no longer be defined regarding military issues and internal and external borders. Still, the risk of reducing citizens' quality of life threatens national security today. Another issue is the disappearance of the geographical dimension of cyber threats because military threats had a specific geographical location in the past. As a result, it was not difficult to deal with, at least in terms of identity. The degree of vulnerability caused by cyber threats is also one of the effects of cyberspace. These scattered threats are multi-dimensional, and due to the connection with sensitive networks and infrastructures, the amount of their damage is very high, and they cannot be contained only by traditional methods such as the use of military and police force; governments alone are not enough to deal with them, and It requires effective and bilateral cooperation between governments and the private sector that have common interests in dealing with them. As the previous point shows, cyber threats are not limited to governments; individuals and different companies are also not immune from the harm of these threats [1].

The reviewed literature shows several gaps that top management and cybersecurity professionals must close to construct a successful digital institution in the conviction- and assurance-based economy. These gaps indicate four factors: top management commitment and support, budgeting, cybersecurity compliance, and cybersecurity culture. The difference between the highest and lowest levels of all 4 factors is very small, and such a small variance shows the importance of all 4 indicators for cyber security awareness. Also, among the practical implications for policymakers and cyber security professionals, it can be noted that the study in cyber security awareness provides a vital factor that may help improve policies or guidelines for successful cybersecurity awareness in organizations [4].

As stated, one of the research gaps in this field is related to investigating the effect of culture on conservation motivation because most of the existing research has focused on technological, organizational, and behavioral factors affecting conservation motivation [5]. A review of existing literature in the field of cyber security culture and awareness showed things such as education [6], Specialist forces [7], Personnel participation [8], trust [9, 10], competence [11, 12], evaluation [13], Threat response ability [14] and commitment [15] play a role in cybersecurity culture and awareness.

Therefore, information security is a challenge facing organizations, as security breaches seriously threaten sensitive information. Organizations face security risks concerning their information assets, which may also stem from their employees. Organizations need to focus on employee behavior to limit security failures, as if they wish to establish an effective security culture with employees acting as a natural safeguard for information assets. Therefore, the existence of a structure in the field of information security culture by covering the factors affecting the security culture and the factors reflecting it in this area can be useful by introducing a comprehensive framework in practice, which contributes to the creation of a security culture, it will help to improve information security management because factors are critical in justifying the adoption of a security culture, and the framework provides an important tool that can be used to evaluation and improve an organization's security culture [16]. Providing a tool, either in the form of a framework or in the form of a scale to evaluate cyber security culture and awareness, is useful when there is confidence in its reliability.

Ensuring the reliability and validity of a newly developed instrument depends on using professional methods in assessing that instrument. For this reason, in this research, an attempt will be made to use new psychometric methods (IRT) to examine the characteristics of a tool that has been recently made regarding cybersecurity culture and awareness [17]. Since the different perceptions of the text of the questions in the same tool among different people can affect its dimensionality, and according to Alperkose & Demirtasli (2012), this is considered a risk for the analysis of multidimensional data because if they are examined in a unidimensional way, it can It leads to a higher error score in estimating the ability parameters and questions on the one hand and reducing the accuracy of measurement and fitting the data with the model on the other hand; as a result, the obtained results will be biased [18].

In fact, in making tests, in a practical way, when we run them for a group of subjects, we should be able to predict their statistical and psychometric properties. Questions should be described through question parameters and subjects through subject parameters so that it is possible to predict each subject's answer to each question. This description should be possible even for similar subjects who did not answer the same questions. This involves predicting phenomena beyond the control of the psychometers, i.e., predicting how people behave in the real world. Using the main problem of Taylor's measurement, if we assume and administer a set of questions to a subject, we need to know how effective each question in this set is in measuring a certain level of ability. None of these can be achieved using classical test theory (CTT) [19]. These limitations led to the formation of another theory about the construction and interpretation of test scores, which is called the "theory of inherent characteristics" (in some cases under the title "Item-Response theory (IRT)"); this theory can determine the position of questions (items) and subjects in a common scale and review of previous researches regarding the tools made related to cyber security culture and awareness, indicates that no research has been done in this way either inside the country or abroad.

For example, Jafari (2021) stated in research that virtual and cyberspace are the most changing environments governing today's activities. The security of cyberspace, the follower of cyberspace, is affected by continuous changes, and because maintaining security in this space is considered one of the important issues in the country's national security, and also due to the lack of synergy between cyber security research institutions in Iran, benefiting from a governance model This space is considered a suitable solution for governance to use all capacities appropriately. Using the data theory method of the foundation and interviews with experts in this field, he concluded that one of the most important propositions in the field of cyber security is the provision of integrated policies through the creation of a technological roadmap and native cyber security products, the concern of security in the country has been institutionalized. Management is committed to the private sector [20].

Eyvazi and Dadashi Chekan (2019), in research through interviews with experts in the field of cyber security, stated that the most important cyberattacks include cyber war, cyberattacks, cybercrimes, cyber espionage, and cyber riots, and to deal with these threats, three levels of security must be They noted that it includes infrastructure security areas, security level in individual and social areas, and security level in national and governmental areas [21].

In a research conducted by Azmi et al. (2021), the findings indicated that security education, training and awareness programs, and information security awareness were found to have a positive and significant impact on Information Security Culture. Additionally, self-reported employees' security behavior partially mediated the relationship between information security awareness and information security culture [22].

Hassan et al. (2021), in research to investigate the technology-organization-environment framework, provided a comprehensive set of factors affecting the cyber security readiness or awareness of organizations and the effects of these factors on the organization's performance (financial and non-financial) by improving organizational security performance. The results showed that Cyber security awareness positively impacts organizational security performance, positively affecting financial and non-financial performance. The newly proposed comprehensive model of factors affecting the cyber security readiness of organizations and the evidence of their importance can guide future research and enhance the current understanding of how organizations can better equip themselves to minimize the occurrence and impact of cyber-attacks [23].

Georgiadou et al. (2021a), in research to the design of a survey aiming at the cyber-security culture assessment of critical infrastructures during the COVID-19 crisis, made a tool that was rooted in a security culture framework layered into two levels, organizational and individual, further analyzed into 10 different security dimensions consisted of 52 domains. An in-depth questionnaire-building analysis focused on the aims, goals, and expected results [24].

Tolah et al. (2021) also stated in research that information security is a challenge facing organizations because a security breach is a serious threat to sensitive information. Organizations face security risks related to their information assets, which their employees may cause. In this research, the culture of information security and the framework of key factors were developed, which included two factors (factors affecting security culture and factors reflecting it). During this exploratory investigation, the findings showed that the framework was valid and had an acceptable fit with the data. This study filled an important gap in the relationship between personality traits and safety culture. It has also improved information security management by introducing a comprehensive framework in practice, which contributes to creating a security culture [16].

Arbanas et al. (2021), in a research by studying the texts and interviewing experts in the field of cyber security, built a conceptual framework and checked its validity using a wide range of methods. In fact, the measurement tool was developed first, and then the validity of the content and structure of the tool was confirmed through experts' opinions. Convergent validity was tested by confirmatory factor analysis, and instrument reliability was tested using Cronbach's alpha coefficient to measure internal consistency. The resulting framework finally included 46 items that described 8 factors that were grouped into 3 categories. These 3 categories were built around technological, organizational, and social issues. This research has contributed to the knowledge culture of information security by developing and verifying a comprehensive framework for evaluating information security culture, which does not respect information security culture in only one aspect but considers its organizational, sociological, and technical components [25].

Given the above, and considering that increasing cyber security is an ongoing challenge for security professionals, research consistently shows that online users are a weak link in cyber security, and particular, behavior and attitudes towards privacy under the influence of culture are compared to other psychological and demographic variables (such as gender and computer expertise); Also, what kind of data people share is derived from their culture, and, culture affects these choices, and in fact, certain personality traits affect user cybersecurity-related behavior in different cultures; All these cases highlight the importance of paying attention to human resources [26]; Therefore, providing a tool to help solve the challenges faced by security professionals in the field of education and awareness related to cyber security in the form of culture building is necessary. Therefore, in this research, we have sought to answer the question, what are the psychometric characteristics of the cyber security awareness and culture assessment scale based on Item-Response theory (IRT)?

2. Method

The current research was applied in terms of purpose and quantitative research based on new psychometric methods (IRT). The statistical population of the present study consists of all the employees of Bank of Iran branches who are working in the year 2022. In this research, because the intention is to analyze the items of a new tool following the psychometric texts in the field of IRT, it is appropriate to consider a large sample size. Hence, the sample size was 1,000 people, with the possibility of dropping the sample. A simple random method was used to collect data from the "Cyber Security Awareness and Culture Evaluation" scale (2022) [17].

3. Instrument

"Evaluation of cyber security culture and awareness" scale (2023): this scale has a self-report form in the form of 34 items, 6 subscales of ineffective human resources (8 items), budgeting and awareness (8 items), capacity building (7 items), Employee position (3 items), information protection culture (5 items) and security behavior and understanding (3 items) are covered and all are scored on a 7-point Likert scale to assess the level of cyber security culture and awareness. Items are rated on a 7-point scale from "strongly disagree" to "strongly agree." In this scale, 14 items have reverse scoring, and the scale's total score can be between 34 and 238. A higher score indicates a higher level of culture and individual awareness towards cyber security in the subscales and the total scale. The initial validity and reliability of this tool, which is native to Iran, has been checked and confirmed by 11 Iranian experts, and the structural validity by EFA and CFA was also checked and confirmed [17].

4. Finding

The study of demographic characteristics showed that the average age of the sample was between 34 and 37 years old, with an employment history of 8 to 11 years. The minimum age was 23 years, the maximum was 52 years, the minimum employment history was 1, and the maximum was 25 years. In terms of gender, the male gender is the most frequent.

Item-response theory (IRT) was used in the specific part of data analysis to examine the Instrument items. In this section, to reduce errors, Multilog software version 7.03 was used for calculations. In the first step, the important presuppositions of the Item-Response theory, i.e., unidimensionality and positional independence, were examined and confirmed. After that, the thresholds were checked, and the discrimination coefficient was calculated for the items related to each factor. Thresholds are the limits between response options, and in this scale, since we have 7 response options for each item (for favorable (Positive) items from 1 (strongly disagree) to 7 (strongly agree) and for unfavorable (negative) items from 1 (strongly agree) to 7 (strongly disagree)) if Let's define options with K; Then we will have k-1 thresholds for each item. Therefore, 6 thresholds are reported for each item in the "Evaluation of cybersecurity culture and awareness" scale. Regarding the discriminative coefficient, the findings showed that items 8, 12, 16, 20, 24, 28, and 34 had the highest discriminative coefficients, respectively.

Table 1. The level of awareness of scale items on the seven points of the θ

Factor	**N of Item**	***θ***						
		+3	**+2**	**+1**	**0**	**-1**	**-2**	**-3**
Budgeting and awareness	1	0.11	0.15	0.16	0.17	0.17	0.17	0.17
	2	0.18	0.27	0.32	0.33	0.32	0.27	0.18
	3	0.11	0.14	0.15	0.16	0.16	0.16	0.16
	4	0.18	0.27	0.32	0.33	0.32	0.27	0.18
	5	0.13	0.15	0.16	0.16	0.16	0.17	0.17
	6	0.18	0.27	0.32	0.33	0.32	0.27	0.18
	7	0.11	0.20	0.26	0.28	0.30	0.30	0.30
	8	0.15	4.38	5.61	5.75	2.25	0.01	0.01
Capacity Building	9	0.11	0.14	0.16	0.16	0.16	0.16	0.17
	10	0.18	0.27	0.32	0.33	0.32	0.27	0.18
	11	0.11	0.12	0.13	0.13	0.13	0.13	0.13
	12	4.40	6.37	8.93	7.30	0.01	0.01	0.01
	13	0.13	0.18	0.21	0.22	0.22	0.23	0.22
	14	0.18	0.27	0.32	0.33	0.32	0.27	0.18
	15	0.07	0.26	0.58	0.38	0.71	0.73	0.63
Security behavior and perception	16	4.40	6.37	8.93	7.30	0.01	0.01	0.01
	17	0.16	0.29	0.36	0.37	0.38	0.39	0.39
	18	0.18	0.27	0.32	0.33	0.32	0.27	0.18
Inefficient human resources	19	0.12	0.36	0.58	0.62	0.63	0.66	0.61
	20	3.80	2.29	8.79	0.69	0.01	4.91	0.02
	21	0.14	0.27	0.36	0.38	0.39	0.40	0.39
	22	0.18	0.27	0.32	0.33	0.32	0.27	0.18
	23	0.12	0.22	0.30	0.32	0.33	0.33	0.33
	24	3.80	6.29	8.79	0.69	0.01	4.91	0.02
	25	0.13	0.35	0.54	0.58	0.60	0.61	0.60
	26	0.18	0.27	0.32	0.33	0.32	0.27	0.18
Employee position	27	0.07	0.27	0.59	0.68	0.72	0.74	0.71
	28	4.38	6.30	5.50	0.01	5.50	6.28	0.02
	29	0.11	0.33	0.56	0.60	0.63	0.65	0.65
Information protection culture	30	0.18	0.27	0.32	0.33	0.32	0.27	0.18
	31	0.07	0.08	0.09	0.09	0.09	0.09	0.10
	32	4.38	6.30	5.50	0.01	5.50	6.28	0.02
	33	0.06	0.08	0.09	0.10	0.10	0.10	0.10
	34	0.18	0.27	0.32	0.33	0.32	0.27	0.18
total		30.01	49.65	61.51	31.70	23.34	32.15	8.75

According to Table (2), items 8, 12, 16, 20, 24, 28, and 34 had the highest level of awareness. Also, the level of awareness of the whole scale on seven points of the theta continuum indicates that the maximum awareness of the scale is between +1 and +2 theta points. The awareness value at +1 theta is equal to 61.508, and the awareness value at 2 theta point is 49.649. The amount of awareness in theta-3 has a minimum.

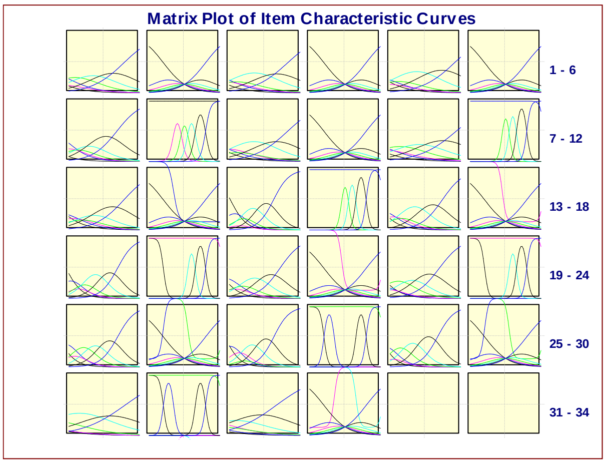

Figure 1. Matrix Plot of Item Characteristic Curves of 34 items of cybersecurity awareness and culture assessment scale

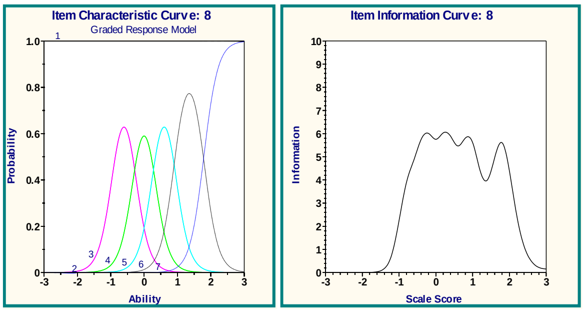

Figure 2. Item Characteristic Curves and θ in one of the good items of the scale (Item no. 8)

Figure (2) shows the curve of the response class and the curve of the θ of one of the good items of the scale (item no. 8) and indicates that this item has a high recognition power throughout the latent trait values and the classes of response options do not overlap to a large extent. The larger the discrimination parameter, the tighter the response floor curves and the higher their height. This shows that the response class determines the difference in trait levels in this type of item relatively well [27]. In other words, the threshold parameters between the classes in the domain of culture and awareness of cyber security in these types of items have a relatively good dispersion.

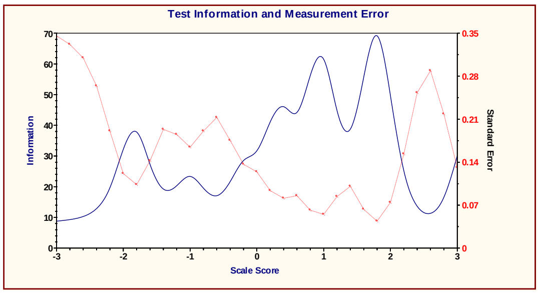

Figure 3. Test Information and Measurement Error for Scale

Figure (3) shows the θ of the whole scale. As it is evident, wherever the θ increases, the error is reduced and vice versa. According to this figure, the highest level of θ is between +1 and +2, and the maximum total θ is equal to 70, which shows the desirability of the entire scale level.

5. Conclusion

The present study was conducted to analyze the cyber security awareness and culture assessment scale based on the Polychotomous models of Item-Response Theory (IRT) and to achieve this goal, using the common Polychotomous model in the IRT theory called the graded response model (GRM), we investigated the coefficient It was possible to identify each item and index, and the findings indicated that the θ status and discriminative coefficient of all 34 items are relatively acceptable.

Considering that the scale examined in the present study had a multi-grade response spectrum, the GRM model was suitable for the analysis of its items because, in this model, each scale item is described by a discriminative coefficient and threshold parameters between classes. Using the GRM model, the position of these thresholds can be determined on the latent trait continuum. Also, by using class response curves (Figure 1), it is possible to show the probability of a person responding in a specific class under the condition of a certain level of the trait. Also, by using category-response curves (Chart 1), it is possible to show the probability of a person responding in a certain class under a certain trait level. The item parameters in the GRM determine the shape and position of the category-response curves. As a result, the larger the discriminative parameters' size, the more compact the category-response curves, and their height is higher. This shows that the category response specifies the difference in attribute levels relatively well.

The threshold parameters between categories Determine the point of elevation of each category-response curve in the middle of the options. Also, the category-response curves rise in the middle of two threshold parameters close to each other. Therefore, it can be said that some of the items in this scale, whose curve is flat, should be removed or revised from the total of items until the category-response curves become more compact. Their height does not increase; the items' revision and analysis should continue to achieve the desired situation regarding the cyber security culture and awareness evaluation scale. We know that the most changing environments governing today's activities are virtual and cyberspace, but due to the lack of synergy between cyber security research institutions in Iran, benefiting from a model for the governance of this space to use all capacities appropriately is considered a suitable solution for governance [20].

On the other hand, the impact of COVID-19 has affected most aspects of society, and cyber security has not been excluded from this issue [11]. In addition, the examination of the model of strategic development of human resources in the field of cyber security of the Armed Forces of the Republic of Iran has also indicated the need for technical and equipment aspects to develop and cultivate competent and efficient human resources [26]. In this regard, to deal with cyber threats, attention should be paid to the three levels of infrastructure security: the security level in the individual and social areas and the security level in the national and governmental areas [21]; Training employees [6] and making them aware of their job position can be effective in improving people's culture and awareness of cyber security because awareness is very important in creating a culture of cyber security [10]. However, this awareness requires training, aligning with the factors affecting cyber security culture to promote culture and awareness [22]. For example, among these factors are employees' understanding [23], their behavior at the workplace, security culture (at both organizational and individual levels) [24], and personality characteristics [9, 16] because increasing the current understanding and awareness of how Better equipping organizations to minimize the occurrence and impact of cyberattacks is fruitful [23] and this issue is included in the framework of the human factor because this factor considers the specific approach of technical, behavioral, cultural and personal indicators and in identifying possible security risks caused by Privileged people help [12]. Therefore, it is important to evaluate human vulnerability in different frameworks to evaluate the cyber security capacity of organizations [9]. This is important with the existence of a valid tool in this field. Therefore, in this research, an effort was made to measure the tool that was developed to evaluate the cyber security culture and awareness in our dear country of Iran [17] using the methods available in new theories to measure the level of culture and People's awareness of cyber security has been measured. In line with that, necessary training and strategies have been conducted to improve and upgrade the existing situation in public and private organizations.

6. Funding

The author of the article would like to thank all the participants in this research, as well as "Dr. Mohammadreza Yekta" for their valuable guidance in the field of cyber security, as well as the "Applied Research Office of Police Command of Isfahan Province" who accepted the organizational support of this project.

7. References

[1] Y. Li. and Q. Liu, “A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments”, *Energy Reports*. vol. 1, no. 7, pp. 8176-8186, 2021, doi: https://doi.org/10.1016/j.egyr.2021.08.126

[2] A. Alzubaidi, “Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia”, *Heliyon*. vol. 1, no. 7(1), pp. e06016, 2021, doi: https://doi.org/10.1016/j.heliyon.2021.e06016

[3] JV. Bino, “Cyber Security Awareness by Using Social Media Platforms Among Students”, *International Journal of Research (IJR)*, vol. 8, no. 5, pp. 581-589, 2021, [Online]. Available:http://ijrjournal.com/index.php/ijr/article/view/51

[4] AI. Al-Alawi. and AS. Al-Bassam, “Assessing The Factors of Cybersecurity Awareness in the Banking Sector”, *Arab Gulf Journal of Scientific Research*. vol. 37, no. 4, pp. 17-32, 2019, doi: https://doi.org/10.51758/AGJSR-04-2019-0014

[5] K. W. HOE, "Culture and cyber security: How cultural tightness-looseness moderates the effects of threat and coping appraisals on mobile cyber hygiene," Doctoral dissertation, Singapore Management University, 2021. [Online]. Available: https://ink.library.smu.edu.sg/etd_coll/357/

[6] M. Sahraei., M. valavi., B. bayat. and A. Taraghi, “Provide a native model of cyber monitoring, monitoring and alerting based on the ooda cycle”, *National Security*, vol. 10, no. 37, pp. 473-512, 2020. [Online]. Available: https://ns.sndu.ac.ir/article_1118.html (in Persian).

[7] F. Tavakoli., M. Mortazavi. and M. Keshavarztork, “Determining Strategic Factors Affecting the Prevention of Cybercrime with Fuzzy Delphi Approach”, *Journal of Social Order*, vol. 12, no. 4, pp.113-140, 2021. [Online]. Available: http://sopra.jrl.police.ir/article_95455.html (in Persian).

[8] I. Progoulakis., N. Nikitakos., P. Rohmeyer., B. Bunin., D. Dalaklis., S. Karamperidis, “Perspectives on cyber security for offshore oil and gas assets”, *Journal of Marine Science and Engineering*. vol. 9, no. 2, pp.112, 2021, doi: https://doi.org/10.3390/jmse9020112.

[9] D. Papatsaroucha., Y. Nikoloudakis., I. Kefaloukos., E. Pallis., E. Markakis, “A Survey on Human and Personality Vulnerability Assessment in Cyber-security: Challenges, Approaches, and Open Issues”, *arXiv preprint arXiv:2106.09986*, 2021. doi: https://doi.org/10.48550/arXiv.2106.09986

[10] B. Uchendu., JR. Nurse., M. Bada., S. Furnell, “Developing a cybersecurity culture: Current practices and future needs”, Computers & Security. vol. 1, no. 109, pp. 102387, 2021, doi: https://doi.org/10.1016/j.cose.2021.102387

[11] A. Georgiadou., S. Mouzakitis. and D. Askounis, “Working from home during COVID-19 crisis: a cyber security culture assessment survey”, *Security Journal*, vol. 35, no. 2, pp. 1-20, 2021, doi: https://doi.org/10.1057/s41284-021-00286-2

[12] A. Georgiadou, S. Mouzakitis, and D. Askounis, "Detecting Insider Threat via a Cyber-Security Culture Framework," *Journal of Computer Information Systems*,

vol. 62, no. 4, pp. 706-716, 2022/07/04 2022, doi: https://doi.org/10.1080/08874417.2021.1903367.

[13] P.R. Trim, Y.I. Lee. "The global cyber security model: counteracting cyberattacks through a resilient partnership arrangement", *Big Data and Cognitive Computing*, vol. 5, no. 3, pp. 32, 2021, doi: https://doi.org/10.3390/bdcc5030032.

[14] K.L. Bethel, "An Evaluation of Organizational Culture: Its Influence on Security Culture: A Case Study", Doctoral dissertation, Northcentral University, 2020. [Online]. Available:https://www.proquest.com/openview/001623eb1e1a44dfce30d35f6555a6b1/1?pqorigsite=gscholar&cbl=18750&diss=y

[15] T.A. Nguyen., K. Koblandin., S. Suleymanova and V. Volokh, "Effects of 'Digital'Country's Information Security on Political Stability", *Journal of Cyber Security and Mobility*, vol. 12, no. 1, pp. 29-52, 2022, doi: https://doi.org/10.13052/jcsm2245-1439.1112.

[16] A. Tolah., S.M. Furnell. and M. Papadaki, "An Empirical Analysis of the Information Security Culture Key Factors Framework", *Computers & Security*, vol. 108, pp. 102354, 2021, doi: https://doi.org/10.1016/j.cose.2021.102354.

[17] S. Heydari., M. Barzegar., A. Mohammad Davoudi, "Factor structure analysis of the scale "Evaluation of cyber security culture and awareness" (case study: bank branch employees in Ahvaz city)", *Psychological Methods and Models Quarterly*, vol. 14, no. 51, pp. 113-126, 2023, https://doi.org/10.30495/jpmm.2023.31055.3716. (In Persian)

[18] M. Ahmadi deh Ghutbuddini, E. khodai, V. Farzad, A. Moghadamzadeh and M. Kabiri, "Applying Bi-factor Multidimensional Item-response Theory Model for Dimensionality and Differential Items Functioning Analysis on Testlet-Based Tests", Quarterly of Educational Measurement, vol. 7, no. 28, pp. 121-153, 2017, doi: https://doi.org/10.22054/jem.2017.22168.1541, (In Persian).

[19] F. M. Lord, *Applications of Item-Response Theory*, translated by A. Delavar. and J. Yunesi, 2011. Tehran, Roshd Publications, 2011. (In Persian)

[20] Z. Jafari, "Cyber security", In Proc. 7th national conference of new ideas in technology and engineering, 2021. [Online]. Available: https://civilica.com/doc/1239064 (In Persian)

[21] MR. Eyvazi and MM. Dadashi Chekan, "Types of threats in the cyberspace and solutions to deal with them", In Proc. second national cyber defense conference, 2019. [Online]. Available: https://civilica.com/doc/903617 (In Persian)

[22] N. A. A. Md Azmi, A. P. Teoh, A. Vafaei-Zadeh, and H. Hanifah, "Predicting information security culture among employees of telecommunication companies in an emerging market," *Information & Computer Security*, vol. 29, no. 5, pp. 866-882, 2021, doi: https://doi.org/10.1108/ICS-02-2021-0020

[23] S. Hasan, M. Ali, S. Kurnia and R. Thurasamy, "Evaluating the cyber security readiness of organizations and its influence on performance", *Journal of Information Security and Applications*, vol. 58, pp. 102726, 2021, doi: https://doi.org/10.1016/j.jisa.2020.102726.

[24] A. Georgiadou., S. Mouzakitis., D. Askounis, "Designing a cyber-security culture assessment survey targeting critical infrastructures during covid-19 crisis", *International Journal of Network Security & Its Applications (IJNSA)* vol. 13, no. 1, pp. 33-50, 2021. [Online]. Available: https://ssrn.com/abstract=3787197

[25] K. Arbanas, M. Spremic, and N. Zajdela Hrustek, "Holistic framework for evaluating and improving information security culture", *Aslib Journal of Information Management*, Vol. 73 No. 5, pp. 699-719, 2021, doi: https://doi.org/10.1108/AJIM-02-2021-0037

[26] H. Kaviani, N. Mirsepasi and G. Me'marzadeh Tehran, "A Pattern for Strategic Development of Human Resources in the Field of Cyber Security of the Armed Forces of Islamic Republic of Iran", *Defence Studies*, vol. 18, no. 1, pp. 37-66, 2020. [Online]. Available: https://ds.sndu.ac.ir/article_1008.html?lang=en (In Persian)

[27] Sh. Vahedi and T. Hajipoor, "Study of psychometric Properties of College Self-Efficacy Inventory among college students using confirmatory factor analysis (CFA) and Item Response Theory- (IRT)", *Quarterly of Educational Measurement*, vol. 4, no. 16, pp. 173-192, 2014. [Online]. Available: https://jem.atu.ac.ir/article_328.html (In Persian)