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

Online ISSN: 2676-3346

OPEN ACCESS

Vol. 6/ Issue 2/ 2023/ pp. 21-26
DOI: 10.22034/IJRRS.2023.6.2.3
Received: 14 August 2023, Revised: 30 August 2023, Accepted: 10 September 2023
Available online at: https://www.ijrrs.com

Original Research Article

Meta-Analysis of the Research Conducted in the Field of Cyber Security with an Emphasis on the Human Circle

Sedigheh Heydari*[1]

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

*** heydari_ss@yahoo.com**

Abstract

The expansion of the use of information has caused communication and closeness between different cultures and their influence on each other, so it can be said that culture is now full of more information than in previous periods. Therefore, information technology has affected cultural values in such a way that even they have been exposed to the challenge of transformation and fundamental cultural changes from the security aspect. On the other hand, with the growth of various research in the field of cyber security and facing a kind of dispersion of information in this field, it is very important to conduct combined research that presents the extracts of the research conducted in this subject systematically and scientifically. The current research aims to quantitatively combine the results of research conducted in the field of cyber security with an emphasis on the human circle and, by using a meta-analysis method and comprehensive meta-analysis software (CMA2), examines the number of 81 articles. In fact, the statistical population of the research is all articles on cyber security that have been published in the last 3 years in reliable domestic and foreign scientific databases. The result of the meta-analysis of 75 variables shows that it covers 5 main variables. Among them, the variables of awareness, culture and infrastructure impact cyber security most. Most research has been done with descriptive-analytical, documentary and secondary analysis methods. The effect size results showed that the variables of awareness (with an effect size of 0.68), culture (with an effect size of 0.61) and infrastructure (with an effect size of 0.42) had the greatest impact on cyber security in the reviewed studies.

Keywords: Meta-analysis; Cyber security; Human circle; Effect size.

1. Introduction

The expansion of the use of information has caused the connection and closeness between different cultures and their influence on each other. It can be said that culture is now full of information more than in previous periods. Therefore, the cultural values, beliefs and behavioral patterns of societies have been strongly influenced by information technology. In such a way, they have been exposed to the challenge of transformation and fundamental cultural changes from the security aspect [1].

In fact, electronic communication features in cyberspace provide users with conditions different from face-to-face relationships. The speed of action, anonymity, etc., provide the same and similar space regardless of requirements such as gender, second class, race and location, creating different user experiences. The interactions that take place in this space create a new mentality and attitude for internet users that can change their behavior and interactions in the real world, however slight [2].

In fact, today, with the birth of virtual space and its rapid growth, we are witnessing that all economic infrastructures and cultural superstructures of societies are changing as if nothing is fixed anymore and everything has become fluid. Perhaps because of these extensive changes, David Bell, a professor at Staffordshire University in England and the author of the book "Cyber Cultures," says the emergence of new communication technologies over the past two decades has brought about profound changes in various fields of daily life. These changes, more than anything else, through changes in communication structures and patterns, have not only affected the culture of contemporary societies but also created a new cultural arena, which with different interpretations is called electronic culture, digital culture, virtual culture, culture Cyber and modern culture have been mentioned. In Iran, where virtual space and social networks have expanded significantly among different strata of people, all cultural, political, social, economic and religious affairs have undergone extensive changes in their existence and meaning [3].

How to cite this article:
S. Heydari. "Meta-Analysis of the Research Conducted in the Field of Cyber Security with an Emphasis on the Human Circle," *International Journal of Reliability, Risk and Safety: Theory and Application*, vol. 6, no. 2, pp. 21-26, 2023.

The emergence of cyberculture, defined by Pierre Levy (1993) as a set of techniques and practices developed and strengthened due to the communities in the virtual space, indicates a violent change in the way societies consume (culture). Its passive position has been replaced by the possibility to participate and issue feedback, transforming online communication channels into two-way and interactive platforms, which are now part of the daily routine of billions of people worldwide [4].

In this regard, the issue of awareness is one of the most important issues in the history of philosophy. Due to the difficulty of defining consciousness, some philosophers have divided it into phenomenal consciousness, access consciousness, self-awareness and supervisory consciousness. Philosophers like Mulla Sadra, who attribute consciousness (science) to the soul and explain the characteristics of consciousness based on this, attribute all types of consciousness to something beyond matter. Therefore, from his point of view, consciousness cannot be reduced to matter [5].

Consciousness and its place in nature is one of the main questions in the philosophy of mind and is closely related to the mind-body issue. There are different explanations about the relationship of consciousness with the natural world, which seems to be placed in the same traditional dualism of physicalism and dualism. While both explanations face problems that have reduced their acceptance, Russell's monotheism claims to have been able to distance itself from this duality, explain consciousness with its unique characteristics, and define its relationship with nature; in such a way that the principle of causality can be justified based on this idea [6].

On the other hand, the analysis of studies that discuss the definitions and characteristics of security culture has shown that this field has no broad definition. Although patterns emerge when examining the boundary between cyber security culture, information security culture, and security culture, there are parallels in the various definitions of identified culture and broader definitions of organizational culture. Nævestad et al. (2018) state that security culture can simply be seen as the security aspects of a broader organizational culture [7].

Reviewing the recent literature on organizational culture, Oh and Han (2020) describe organizational culture as whether employees are willing to participate in organizational learning activities, and this question confirms Nel and Drevin's (2019) conclusion that safety culture Cyber is not only an organizational subculture but ultimately culture should become a part of organizational functions. From this point of view, it is clear why many definitions refer to organizational culture and its important role. Therefore, an important point is that security cultures should complement broader organizational culture efforts [8].

Regarding the description of cyber security culture, we find that organizational expectations are the same across industries and are often related to how employees behave in the workplace and are reflected in definitions and across domains of security culture. For example, Hasan and Ismail (2016) define information security culture as employees describing information security as a natural part of their daily organizational tasks when related to healthcare settings [8].

Masrek et al. (2018) conducted their work in the public sector context and stated that employees should know about information security in organizations with policies to protect protected information [9].

In the study conducted by Marotta and Pearlson (2019) in the context of a large bank, cybersecurity culture was described as the attitudes and values that encourage cybersecurity behaviors in the organization's employees, and in another definition by Wiley, McCormack, and Callick (2020) stated, cybersecurity culture is described as a subculture of organizational culture that includes the attitudes, beliefs, values, and knowledge that individuals use to interact with organization systems and perform related daily procedures, tasks, and activities. Mainly, this definition describes culture as normal behavior in organizations [10]. The similarities between these definitions across industries and domains show that, regardless of context, organizations and their employees are expected to perform certain protective behaviors and follow existing procedures to meet security culture expectations when examining the criteria used to measure security culture. Cyber, the most obvious detail is that questionnaires and surveys are the main means of measuring knowledge or security policy awareness. While these techniques cannot be underestimated, and despite their dominance in the literature, these methods create challenges for organizations [8] because security awareness is an awareness and adaptation that comes from a deeper process that leads to a culture of security. Strong cyber needs to be cultivated through a long and hard procedure that requires organizational and individual participation [11].

Therefore, considering that security is one of the most important social, cultural and psychological components of any society and according to the field of sociological and psychological studies, this component is necessary for the life of any political and social system. Therefore, the issue of security, especially cultural security in the virtual space, is influenced by many economic, political, social and cultural factors. As a traumatic phenomenon, it has always caused the decrease and fading of the sense of security among societies [1].

Concerning the mentioned materials, in the period of the outbreak of COVID-19, when the world continued the way of business and education, etc., the issue of cyber security was also raised as one of the most common research topics and was investigated by researchers. It has been placed many times. These researches are often conducted in different statistical communities and based on various theoretical frameworks and models. But what

is noticeable about most is the extent and dispersion of the investigated indicators in each study, which varies according to the investigated area. Each of these researches has chosen different variables, patterns and models.

Therefore, reviewing the research conducted in the field of cyber security to know the dominant conceptual and operational framework, models and patterns used in each of the research is the main goal of this article so that through this, the most meaningful assumptions and concepts used in the researches to examine the situation Cyber security should be extracted and combined. In the following, after a general overview of the cyber security literature, the explanation of the application of meta-analysis in combining the results of cybersecurity-related research with an emphasis on the culture and awareness of the human circle will be discussed. Then, the findings of the meta-analysis will be discussed. This article tried to answer the question: What variables have been studied in cyber security research, emphasizing the human circle?

2. Method

Meta-analysis is the process of statistically combining the results of independent and separate researches to reach general results about what the research background shows. Since 1930, statisticians and methodologists have used various methods to perform a meta-analysis, a general classification divided into three categories: critical factors approach, Bayesian approach and results combination approach. Among the mentioned methods, the approach of combining the results has gained more acceptance because it benefits from strong statistical tests for the quantitative combination of the results. As mentioned earlier, the oldest statistical test examines the results of studies using the T-value. Although this method has disadvantages and limitations, it is still considered one of the best tests for combining results. One of the most basic concepts in meta-analysis literature is the concept of effect size. In a comprehensive statistical definition, the effect size is the ratio of the significance test to the volume of the study, and the effect size indicates the extent or degree of the phenomenon's presence in society. The larger the size of the effect, the greater the phenomenon's presence [12].

Meta-analysts can calculate the effect size by having groups' mean, variance and standard deviation. Still, the most common statistics in this field are r and d, which usually use d for group differences and r for correlation studies. In this research, the meta-analysis method used, according to the nature of the data, is in the category of quantitative research. In terms of its purpose, it is included in the applied research group. The subject of this research is the articles related to cyber security during the period of the outbreak of Covid-19. Articles that have been printed and published in electronic form have been used. In fact, to carry out the present research, the collection of articles published inside and outside the country in the field of cyber security from the winter of 2020 to the winter of 2022 (since the outbreak of COVID-19), with an emphasis on the human circle and 3 keywords (cyber security, human factors) were collected in reliable databases[1].

In this meta-analysis, the results of studies studied that have met the necessary conditions from a methodological point of view, including the criteria for entering articles into the research, applicable content for the research question and studies related to the target variable, and the exclusion criteria for abstracts of articles, book chapters, Company reports and lack of access to the full text of the article.

To collect the data required for meta-analysis, a coding form was used. This form was equivalent to the questionnaire or interview form in other types of research. The information in this form has been analyzed to perform calculations using comprehensive meta-analysis software (CMA2). This work was done using the effect size calculation technique. This way, the statistical tests used in the hypotheses were analyzed after being converted into the effect size. In this research, the funnel plot method was also used to measure the publication bias, Duval and Tweedie's and safe N methods was used to determine the number of missing studies, and the heterogeneity test was used for the presence of moderating variables. They have been mentioned.

3. Finding

3.1 Descriptive

In this article, the focus has been on the human circle because the behavior of humans in the cyber domain greatly impacts cyber risks. For this reason, articles referring to technical issues, non-human structure and technology were not considered. Therefore, the number of articles was reduced to 81 articles. Out of a total of 81 reviewed articles, 62 articles were qualitative with a literature review, and 19 were quantitative or mixed. The statistical population studied in these articles included more than 7415 employees and managers of different organizations and even students. Teachers had an average of 390 people for each study, and their statistical sample size was equal to 3471 people and 46.81% of the statistical population, with an average of 183 people for each study.

Regarding the sampling method, 68.42% used the simple random method, 10.53% used the cluster method,

1. For example: https://www.sid.ir/fa/journal/, www.ensani.ir, www.magiran.com, https://www.noormags.ir/, www.civilica.ir, https://scholar.google.com/, https://www.scopus.com/home.uri, https://link.springer.com/, https://sci-hub.se/, https://www.ieee.org/, https://www.sciencedirect.com

15.79% used the stratified method, and 5.26% of the studies did not mention the sampling method.

The research results show that the validity of the measurement tool in 78.95% of the articles was only the opinion of the professors and experts in the related field, and only 21.05% was discussed using factor analysis. Concerning validity, the findings indicate that Cronbach's alpha method was used in 89.47% of the articles, and the average coefficients obtained were 0.83. In the rest of the cases, this importance was not mentioned. In all the articles, the type of research is mentioned in terms of practical purpose, and their research method was 15.79% correlation method and 84.21% descriptive-survey method. Regarding the 62 qualitative articles conducted in the form of literature review, the type of basic research and its method were content analysis and text analysis.

In general, the number of 965 variables identified in the studies in question can be summarized under the title of 75 variables, considering the repetition and the fact that in some studies, it is used as an independent variable and in another study as a dependent variable. Five general variables are culture, awareness, infrastructure, budgeting and capacity building. Therefore, the variables of interest in the 81 researches that affect cyber security with an emphasis on the human circle include political systems; social and organizational effects; Implementation of security policies and new approaches in education; lack of up-to-date and efficient laws; Predominance of strict thinking in the judicial system; lack of planning and policy in the field of virtual space; lack of transparency in the structure and function of governance and government; work experience; insider threat; personality talents; Expertise work experience; teamwork and group work; Personality characteristics; Incomplete socialization of social-family capital erosion; lifestyle changes; social failures; Improper management of free time; cultural poverty; mental-psychological problems; Inadequacy of manpower with work, low culture of using virtual space; Weak knowledge of employees; ineffective human resources; Lack of preparation; lack of experience; specialized forces; personnel participation; work processes and behavior prioritization; stressful events and economic hardships; economic systems; Problems with the technical structure of virtual space; technical infrastructure planning; Capacity Building; training programs, security program management and user security management; Budgeting support for user training; allocation of resources; Customizing the needs of employees and the organization; integration of electronic and physical learning resources; prevent hacker penetration; thoughts and beliefs; The unattractiveness of internal programs; Competence of employees; Assessment; Ability to respond to threats, commitment; Understanding the security risk; Human-related cyber threats; human-related security factors; social engineering; the trust; the behavior of members, especially the behavior of managers; the behavior of work groups; security behavior; emotional stress; emotions; internal and external motivation; Dissatisfaction of employees with work pressure, use of smartphones and not observing security considerations at work; Unsafe use of e-mail; Poor computer and account security; Using USB and personal devices; remote access and work at home; lack of encryption; Poor update; poor physical security; poor backups, IT sabotage; new ways of sharing information, not being familiar with the current topics of new technologies; security awareness; Ignorance and low level of awareness.

Among the most important concepts related to the cyber security category (with emphasis on the human circle) and have been repeated in various research, we can mention awareness, culture and infrastructure.

3.2 Meta-Analysis Findings

Table 1 reflects the distribution of 75 items of effect size that explain the relationship between variables and dimensions of cyber security (with emphasis on the human circle).

Table 1. Frequency distribution of effect size classes of cyber security variables and dimensions

The scope of changing the intensity of the effect	Frequency	%
Impact intensity below 0.3 (low)	5	6.67
Between 0.3 and 0.5 (average)	23	30.66
0.5 and above (high)	47	62.67
sum	75	100.0

According to Table (1), out of 75 variables, 5 items, equal to 6.67%, are in the low class, 30.66% are in the middle class, and finally, 47 items are equal to 62.67% in the high class. In addition, the examination of 3 variables out of 75 identified variables showed that the variables of awareness (with an effect size of 0.68), culture (with an effect size of 0.61) and infrastructure (with an effect size of 0.42) have the greatest impact on cyber security. In the reviewed studies and based on the upper and lower limits of the effect size suggested by Cohen (1988) (small: 0.1-0.3; medium: 0.3-0.5 and large: 0.5-0.8), The effect size obtained in the first period is small, and the studied hypothesis is not strong enough.

Also, when the value of r is in the second interval, the effect size is moderate. Finally, when the value of r is in the third interval, the intensity of the effect is evaluated as high. According to this classification, less than 10% of the effect sizes in the present study are in the low category, and this means that approximately 10% of the variables do not have sufficient strength, and their influence and influence on each other will be weak. Also, the size was equal to or greater than 0.3 in about a third of the effects. Based on the effect size proposed by Cohen, the variables of this group are stronger and more reliable than the previous group, and finally, about 60% of the variables (more than half of them) are placed in the third class. These variables have very high reliability, which means that by examining and retesting these

variables, it is very likely that their influence will be confirmed.

One of the issues of concern in any meta-analysis is the assessment of publication bias. Publication bias means that a meta-analysis does not include all studies on the topic under review. For various reasons, some studies may not have been published, or at least in non-indexed journals. When there is publication bias, the final results of the meta-analysis will be affected, and the resulting final estimates will have bias and error. Therefore, it is necessary to identify and correct the publication bias in the initial steps of a meta-analysis to increase the results' validity [12].

The most common and simplest method of identifying diffusion bias is to use a two-dimensional scatter diagram called a funnel diagram, in which the intervention effect estimated from each study is plotted against the study's sample size. The graph is expected to be symmetrical if there is no diffusion bias. The funnel diagram of the present study indicated the absence of publication bias. Duval and Tweedie have developed a correction and fitting method to assess and adjust for publication bias in small samples. This method uses an iterative process in which non-matching observations are removed from the funnel plot (removal of outliers from the distribution). The values assigned to missing studies are added. That is the act of filling in the estimate of the effect size and the standard error of the studies that are probably missing. The occurrence of many missing studies on one side of the effect mean line indicates publication bias or small sample bias. Table (2) shows Duval and Tweedie's correction and fitting method results.

Table 2. Table 2. Modification and fitting of Duval and Tweedie's

	Fixed effect			**Random effect**		
	Point estimation	**lower bound**	**upper bound**	**Point estimation**	**lower bound**	**upper bound**
The value of observations	0.65	0.62	0.68	0.66	0.59	0.73
Adjusted value	0.65	0.62	0.68	0.66	0.59	0.73

According to the data in Table (2), the observed value of 0.65 with the adjusted (corrected) value of 0.65 in the fixed effect model and the observed value of 0.66 with the adjusted (corrected) value of 0.66 in the random effects model, approximately Equal to.

Table 3. Error-safe N computations (classical safe integers)

Indicator	**value**
z value for observed studies	42.035
P value for observed studies	0.001
α	0.05
remainder (sequence)	2
Z for α	1.96
N of the studies viewed	78
N of missing studies that would increase the P value to α	3751

According to the data in Table (3), another 3751 studies should be added to the studies so that the P value of the two domains does not exceed 0.05. This means that 3751 more studies should be done for an error to occur in the final results of calculations and analyses, which shows the high precision and accuracy of the information and results obtained in this research. The number of 3751 studied cases is a reasonable and significant value. Also, considering that the significance level obtained is less than 0.05 ($P<0.05$) and less than 0.01, with 99 percent confidence and an error of less than 0.01 ($P<0.01$), the opposite hypothesis, which indicates the existence of a significant difference between the effect sizes, has been obtained; approved.

Considering that quantitative, qualitative and mixed articles have been examined in this research, this heterogeneity of findings indicates the existence of a moderating variable that has affected the results of the study on the obtained variables. In such a situation, meta-analysts should check the intervening variable or variables that this heterogeneity may have occurred due to their possible influence. In the current research, because the characteristics of the statistical samples of the studies in question were not completely separated and transparent, it was impossible to divide the studies into subgroups based on the moderator variables. Therefore, the researcher faced limitations in identifying the moderating variables.

4. Conclusion

This article aims to investigate and identify those variables that have been used in cyber security research, emphasizing the human circle. In fact, an attempt was made to review the articles that target the human circle. The considered period was the period of the Covid-19 outbreak. This period was targeted because of the significant increase in human activity due to remote work and other related issues, which paralleled the cause of increased cyber risks. According to the meta-analytic findings of the present study, the influence of the variables that were placed in the first category, such as backup, physical security, and dissatisfaction with work pressure, on cyber security is not strong enough, and the possibility of not confirming these variables in similar studies is high. Also, variables such as culture, awareness and infrastructure factors were placed in the middle and upper middle class, which is more important according to the effect size suggested by Cohen.

These results strengthen the findings of previous research. For example, in the study done [11], Culture and awareness of cyber security were reported as effective variables. Security awareness is awareness and adaptation that comes from a deeper process. This category needs to cultivate a strong cyber security culture [11]. Considering that security is one of the most important social, cultural, and psychological components of any society, and according to the field of sociological and psychological

studies, this component is necessary for the life of any political and social system. Therefore, the issue of security, especially cultural security in the virtual space, is influenced by many economic, political, social and cultural factors, and it has always been a harmful phenomenon that has caused a decrease in the sense of security among societies [1].

However, although conducting various tests in the field of effect size measurement, publication bias and homogeneity test shows the accuracy and correctness of the research findings, the existence of moderating variables is considered one of the findings of this research. The current research is insufficient due to insufficient information Obtained from previous research and the lack of separation of quantitative and mixed articles from qualitative articles; it has not been identified. Therefore, it is suggested that in future research, this separation should be done, and the moderating variables should be identified Because this is considered one of the inherent limitations of this research.

5. References

[1] S. Sharifi Rahnmo., A. Fathi., E. Emrani., M. Sharifi Rahnmo, B. Zare kohan., M. Ebrahimi, M. "Forecasting Components of Youth Cultural Security based on the Degree of Attachment to Cyberspace", *Societal Security Studies*, vol. 12, no. 65, pp. 69-88, 2021, doi: 20.1001.1.23224347.1402.11.1.6.7 (In Persian).

[2] M. Ezzatzadeh, "Cyber Social Networks and Cultural Development", *Journal of Iranian Social Development Studies*, vol. 13, no. 49, pp. 81-91, 2021, [Online]. Available:https://jisds.srbiau.ac.ir/article_17059.html?lang=en (In Persian).

[3] A. Mohebbi, A. Kia, "Social Networks and Cultural Changes among Students of Universities in Tehran Based on Inglehart's Materialisticand Post-Materialistic Values", *Journal of Culture-Communication Studies*, vol. 21, no. 51, pp. 63-90, 2020, doi: 20.1001.1.20088760.1399.21.51.3.7 (In Persian).

[4] L. Cardoso., M. Castanho, "A cyberculture study: K-pop and the new media-BTS and Twitter", *European Journal of Social Sciences Studies*, vol. 9, no. 6, pp. 1-6, 2021, doi: http://dx.doi.org/10.46827/ejsss.v6i6.1127

[5] Z. Salahshur Sefidsangi, "Analysis of the Notion of Consciousness Mulla Sadra's perspective and connectionism", *Contemporary Wisdom*, vol. 10, no. 2, pp. 133-153, 2020, doi: 10.30465/cw.2020.4605 (In Persian).

[6] N. Shahinnia., I. Azadegan, "Explaining consciousness from Russell's monotheistic perspective and evaluating its effectiveness in responding to the mind-body problem", *Mind Quarterly*, vol. 18, no. 71, pp. 51-82, 2017, [Online]. Available: https://zehn.iict.ac.ir/article_28115.html (In Persian).

[7] T.-O. Nævestad, S. F. Meyer, and J. H. Honerud, "Organizational information security culture in critical infrastructure: Developing and testing a scale and its relationships to other measures of information security," *Safety and Reliability–Safe Societies in a Changing World*, pp. 3021-3029, 2018. [Online]. Available:https://www.taylorfrancis.com/chapters/oa-edit/10.1201/9781351174664-379/organizational-information-security-culture-critical-infrastructure-developing-testing-scale-relationships-measures-information-security-n%C3%A6vestad-frislid-meyer-hovland-honerud

[8] B. Uchendu., JR. Nurse., M. Bada., S. Furnell, "Developing a cybersecurity culture: Current practices and future needs", *Computers & Security*. vol. 1, no.109, pp. 1-38, 2021, doi: https://doi.org/10.1016/j.cose.2021.102387

[9] MN. Masrek., QN. Harun, NZ. Sahid, "Assessing the information security culture in a government context: The case of a developing country", *International Journal of Civil Engineering and Technology*, vol. 9, no. 8, pp. 96-112, 2018, [Online]. Available: https://iaeme.com/Home/article_id/IJCIET_09_08_011

[10] A. Wiley., A. McCormac., D. Calic, "More than the individual: Examining the relationship between culture and Information Security Awareness", *Computers & security*, vol. 1, no. 88, pp. 1-8, 2020, doi: https://doi.org/10.1016/j.cose.2019.101640

[11] 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*, vol. 13, no. 1, pp. 33-50, 2021, doi: https://doi.org/10.5121/ijnsa.2021.13103

[12] V. Ghorbanzadeh., S. Behfar, "Meta-analysis of research on electronic readiness of organizations in Iran", *Smart Business Management Studies*, vol. 2, no. 6, pp. 1-22, 2014, doi: https://ims.atu.ac.ir/article_1175.html?lang=fa (In Persian).