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

Online ISSN: 2676-3346

OPEN ACCESS

Vol. 6/ Issue 1/ 2023/ pp. 63-69
DOI: 10.22034/IJRRS.2023.6.1.7
Received: 13 June 2023, Revised: 27 July 2023, Accepted: 02 August 2023
Available online at: https://www.ijrrs.com

Original Research Article

Ranking of Factors Affecting Cyber Security

Ashkan Kazemi[1] and Sedigheh Heydari [2*]

1. Iranian Social Security Organization, Shiraz, Iran

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

*** heydari_ss@yahoo.com**

Abstract

Considering the nature of cyberspace as the main information base of the country and the possibility of harming it is very likely, it is necessary to take a special look at the issue of cyberspace security, especially at the level of national applications, because the main infrastructure of the country is located in this space. The emergence of any security problem will cause a serious threat to the national security of the country. Therefore, in this research, cyber defense in the social security organization was investigated by aiming to rank the factors affecting cyber security among the employees of the social security organization of Shiraz City in 2023, one of the country's largest organizations. The research findings indicated that six factors of budgeting and awareness, security behavior and understanding, employee position, capacity building, inefficient human resources, and information protection culture are effective on cyber security, among which the most important factors are inefficient human resources, Employee position, and information protection culture. Therefore, attention to these factors is recommended to the relevant officials, and it is suggested to hold training classes to inform and empower the personnel in this area.

Keywords: Ranking; Cyber Security; Social Security; Staffing.

1. Introduction

The emergence and development of information and communication technology led to a cyber phenomenon. This phenomenon quickly covered the public and private space of society. It significantly impacted the military, economic, political, cultural-social, foreign policy, and information diplomacy in its special and general sense, private and public rights, and each country's passive defense field. Put country, but the rapid growth of this phenomenon caused the security of this space to be neglected, and most experts pay less attention to it in explaining this development [1]. But considering the nature of cyberspace as the main information base of the country and the possibility of harming it is very likely, it is necessary to take a special look at the issue of cyberspace security, especially at the level of national applications, because the main infrastructure of the country is located in this space. The emergence of any security problem will cause a serious threat to the national security of the country [2]. Therefore, considering the ever-increasing rate of use of cyberspace in the current world, both at the macro level (government and governance affairs) and at the micro level (among citizens), one of the most important duties of the legislator in this context is to provide security, both civil and it is criminal. Committing a crime or any fraudulent operation in this space changes daily with technology development [3].

According to the expert of the Research Institute of Communication and Information Technology (2019), the intermingling of cyberspace with people's lives has inevitably put the necessity of a secure vital infrastructure on the must-do list of organizations so that we do not witness the impact of cyber threats. The cyber defense project of the National Information Network is also keyed on the same basis. This annex is a document that specifies the framework, requirements, and indicators for evaluating and improving cyber defense for the National Information Network Plan. The National Information Network is the communication infrastructure, the cyberspace of the country, and the term cyber defense, which was approved by the Supreme Council of Cyberspace in 2017, is considered a fundamental and very enlightening key in the document explaining the requirements of the National Information Network.

In fact, cyberspace is a global domain in the information environment that includes interconnected networks, including the internet, telecommunication networks, computer systems, processors, and controllers. Due to the increasing penetration of information and

How to cite this article:
A. Kazemi and S. Heydari. "Ranking of Factors Affecting Cyber Security," *International Journal of Reliability, Risk and Safety: Theory and Application*, vol. 6, no. 1, pp. 63-69, 2023.

communication technology in various areas of societies, organizations, and businesses, maintaining and improving the security of cyberspace is of great importance. Considering the role and position of active organizations in the defense sector, this matter is of great importance because it directly affects the country's national security. The statistics provided by reliable national and international sources show the lack of integration of activities in this field, the lack of alignment and convergence of goals and policies, and in general, the lack of sufficient attention to the security of cyberspace and, as a result, the country's serious vulnerability in this field [4].

On the other hand, due to the ever-increasing developments in various fields, especially in information technology and control systems, all people's daily needs are inevitably tied to industrial developments. On the other hand, the war has left its traditional state and has become a modern war, known as a soft war, considered one of the four main threats to national security in advanced countries. Many events caused by unintentional failures may affect the normal operation of these systems [5].

Cyber security is an important component of the country's infrastructure. Success in cyberspace security depends on a country's ability to protect its proprietary information and data from individuals, entities, and countries that intend to misuse it. A strong cyber security strategy can provide a suitable situation against malicious attacks designed to access, change, delete, destroy, or capture users' or organizations' systems and sensitive data. Cyber security is also useful in preventing attacks that disable or disrupt device or system operations [6].

According to AFTANA [7], in the last six months of 2023, the amount of hacking into user accounts in Iran has increased by 98%. The new report of the Surf Shark company also shows that since 2004, nearly 15 billion internet users worldwide have been cyberattacked. More than 30% of all cyber intrusions worldwide have been made to America and Russia, and Iran is ranked 11th in the world with 159 million intrusions. In comparison, hacker penetration into Iran has grown 98% over the past six months [7].

The Center for Political and International Studies of the country (2022) has also reported that we are currently witnessing various types of cyberattacks; the first type of cyberattack was in the field of infrastructure, an example of which was the Stuxnet attack in 2010 the country's nuclear facilities in Natanz through A malware (known to security experts as a type of worm called Stuxnet) This virus was designed with the cooperation of the United States and Israel to infect about 60,000 computers. Attack on the country's oil and nuclear systems in 2012; Attacking the website of the National Statistics Center and the website of the National Document Registration Organization in June 2016; The theft of the information of about 20 million Irancell subscribers in 2016; attack on the fuel system and oil product distribution points in the Autumn of 2021; Aiming for the system of the Ministry of Culture and Islamic Guidance in April 2022; attack on Tehran's municipal system in June 2022; and The attack on the infrastructure of Evin prison cameras and the infrastructure of Mahan Airline in 2022 are other prominent examples of cyberattacks in the country [8].

In fact, Iran is at the top of the countries using the Internet in the Middle East, and the penetration rate of Facebook among users is 68.5%. The available statistics in 2017 show that while the number of internet users worldwide is 4 billion and 388 million people with a penetration rate of 67%, in Iran, with a population of more than 82 million people, more than 67 million people use the internet and the Internet penetration rate in our country is estimated at 82%. For years, experts in the field of cyber security in Iran have noticed cyberattacks and have given the necessary warnings to relevant institutions. In this regard, it is necessary to increase the security factor of cyberspace and prevent cyberattacks [9].

Like other organizations, the social security organization, which is one of the important service organizations in the country, is at risk of cyberattacks. Therefore, it requires useful human resources to perform well in this field. The social security system is considered a basic prerequisite for economic, social, and cultural development in every country and a lever with the importance of establishing social justice in the civil societies of the world [10]; Therefore, ways to improve performance and try to reach the ideal situation are the challenges facing this organization [11].

According to the information posted on the main portal of the Social Security Organization, the history of measures aimed at the realization and gradual formation of the "Social Security System" in Iran goes back to the approval of the first national employment law in 1922, during which, for the first time, a minimum mechanism for the retirement of employees A government was created. Later developments, including the approval of the "Legal Bill of Workers' Social Insurance" at the end of 1952 and during the prime ministership of Dr. Mohammad Mosaddegh and the establishment of an independent organization called "Workers' Social Insurance Organization", finally the approval of the "Social Security Law" in July 1975 and the formation of " "Social Security Organization" resulted, which can be seen as the beginning of a new evolution in the country's social security system [12].

It has been reported in this portal that after the victory of the glorious Islamic revolution in 1978, the effort to distribute public wealth fairly, along with respecting the principle of individual property, has been manifested in several principles of the constitution, especially in principle 29, and having "social security" as It has been recognized as one of the fundamental rights of citizens, regardless of ethnic, gender and racial differences, and as a duty of the government towards the

people. The social security organization, established by the law approved in 1975, is currently the most important and central organization active in the field of social insurance and retirement in the country; It has covered the largest number of insured retirees and pensioners under its various protections [12].

Today, in countries economies, the quality and combination of expert and capable human resources with basic and key capabilities and skills required for the labor market are considered among the most important institutions determining economic growth and development [13]. On the other hand, competency-based human resource management will be a strong tool that emphasizes people's behaviors and contributes to organizational success [14].

According to the research of the researcher, not only during the period of Covid-19 but also in the last ten years and even before that, no research has investigated the cyber security of the Social Security Organization as an important organization in the country; while this organization It is one of the organizations that has many connections with the public. Even though the social security organization, with more than half a century of activity history, is considered the most extensive institution in the supply of the social insurance system due to its greater connection with the country's population and provides a wide range of quantitative and qualitative services to the main insured and It provides people covered by them [15]; Most of the researches related to this organization are in the field of employee performance [16-19], job satisfaction [20] or organizational justice and trust [21], and none of them have specifically focused on the cyber security of the organization.

In general, cyberspace, as an emerging phenomenon in human life, is the product of the global Internet network, which enables the collection, concentration, transfer, processing, and use of information using information technology between Internet users and virtual space actors worldwide [22]. Considering that the social security organization covers the health and insurance information of a large number of Iranian society, therefore from the point of view of the authors of this article, It is important to prioritize the factors that threaten the release of this information by the employees of this organization. On the other hand, the review of the literature in this field indicates the absence of similar articles in this field, and despite the efforts of the authors of the article, only one research was found. This research that purpose of this was "identify I.R.I Army general staff cybersecurity effective factors," The results indicate that intra-organizational factors, including securing equipment, networks, and software, monitoring cyber incidents and timely response to them, and improving the cyber knowledge of employees and external factors including man-made and natural cyber threats, are I.R.I Army cybersecurity effective factors [23].

In the other research to identify the Factors Affecting the Culture and Awareness of Cyber Security Using Theme Analysis, Findings showed a review of 392 themes identified the basic themes related to cybersecurity culture and awareness, of which 12 themes were asset organizing, continuity, access, and trust, operations, protection, security governance, attitude, behavior, competence, commitment and support, cyber security and they covered the budget. The identified factors can be used as analytical tools in assessing the culture and awareness of cyber security, which is an important factor in the occurrence of cybercrime, logically and morally, to reduce cybercrime and solve related problems in the economic field. Educational, security, social, and cultural payments [24]. In another research that was studied by bank employees (Employees of Bank branches in Ahvaz City), six factors of inefficient human resources, budgeting and awareness, capacity building, employee position, information protection culture, and security behavior and understanding were identified as effective factors in cyber security of the organization [25]. Then, the present study was conducted to rank the factors affecting cyber security culture and awareness using cyber tools.

2. Method

The current research is of the quantitative research type. In terms of practical purpose, in terms of method, it relies on correlation methods and in terms of library and field collection methods. The statistical population of this research is all the employees of the Shiraz social security organization, and the statistical sample is 230 employees of this organization who were working in 2023 and were selected by simple random method.

As described below, a 6-factor scale was used to identify the important factors [26], and structural equation modeling was used to rank the factors. This model prioritizes factors based on t-value and standardized factor load. The adequacy of these factors is also checked using fit indices (the mentioned items are reported in the findings section).

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 total scale score can be between 34 and 238, and a higher score indicates a higher level of culture and awareness of the individual towards cyber security in the subscales and the total scale [26].

4. Finding

The findings of the demographic characteristics of the sample showed that the average age of the participants was 27.64 ± 6.59, the minimum age was 21, and the maximum age was 46. Of the participants, 19.6% were male, 80.4% were female, 5.8% had an associate degree, 73.5% had a bachelor's degree, 14.3% had a master's degree, and 6.3% had a doctorate level. In the examination of the total score of the research variables, the factor of budgeting and awareness has an average of 43.91 ± 5.35; Capacity building factor has an average of 36.73 ± 4.83; The security behavior and perception factor has an average of 17.18 ± 1.82; Inefficient human resources factor has an average of 43.20 ± 6.45; The employee position factor had an average of 15.95 ± 2.52 and the information protection culture factor had an average of 26.66 ± 3.95. Examining the data distribution using the Kolmogorov-Smirnov test indicated that the significance level of the test statistic was not less than 0.05 for any of the 6 investigated factors; hence the assumption of normality of the data distribution was met.

Table 1. Factor load report of factors related to cyber security

Factor	Standardized load (β)	Cronbach α
Budgeting and awareness	0.64	0.70
Security behavior and perception	0.66	0.73
Employee position	0.89	0.77
Capacity Building	0.79	0.71
Inefficient human resources	0.93	0.79
Information protection culture	0.80	0.70

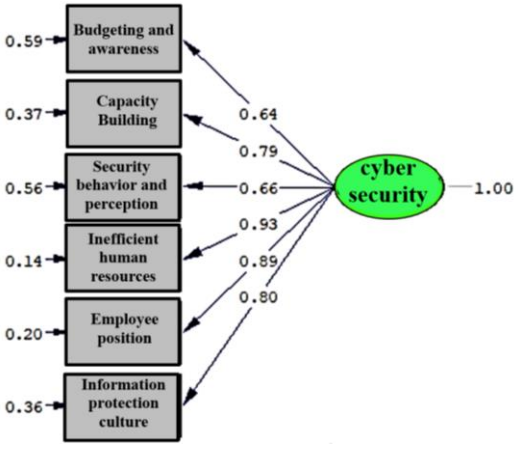

Figure 1. Factor model of factors related to cyber security

According to the table and Figure (1), the factor load for all 6 factors is higher than 0.3, the highest load is for the ineffective human resources factor (0.93), and the lowest load is for budgeting and awareness (0.64). In general, considering that all 6 factors had a factor load higher than 0.3, It can be said that according to the employees of Shiraz Social Security Organization, all factors (budgeting and awareness, security behavior and understanding, employee position, capacity building, inefficient human resources, and information protection culture) are effective in the cyber security of the organization.

Table 2. Model fitness indices

Type of indices	indices	value obtained	Acceptable value
Absolute fit indices	CMIN	45.10	-
	p	0.001	-
	RMSEA	0.064	Less than 0.08
	SRMR	0.073	Less than 0.10
	GFI	0.91	At least 0.90
Incremental fit indices	CFI	0.96	At least 0.90
	IFI	0.93	At least 0.90
	NFI	0.89	At least 0.90
	NNFI	0.92	At least 0.90
Parsimonious fit indices	CMIN/DF	5.01	Less than 6

Table (2) shows that the fit indices, except for the NFI index, have shown favorable values. Suppose at least 3 fit indices are within the acceptable range, and on the other hand. In that case, three important indices of relative chi-square (x2/df), root mean square error of approximation (RMSEA), and the square root of the difference between the residuals of the standardized sample covariance matrix (SRMR) are within the standard range, the fit of the model can be confirmed. Therefore, the current model is approved.

Table 3. Investigating the correlation and ranking of factors based on T values with reporting the mean and standard deviation

Factor	1	2	3	4	5	6	$\bar{x}$	*SD*	T value	Rank
Budgeting and awareness	1						5.49	0.67	10.64	6
Security behavior and perception	0.212**	1					5.73	0.61	11.04	5
Employee position	0.506**	0.696**	1				5.32	0.84	17.06	2
Capacity Building	0.651**	0.545**	0.716**	1			5.25	0.69	14.20	4
Inefficient human resources	0.575**	0.575**	0.833**	0.730**	1		5.40	0.81	18.22	1
Information protection culture	0.692**	0.521**	0.665**	0.556**	0.767**	1	5.33	0.79	14.29	3

*Note: ** p value <0.01*

After confirming the fit of the model; to prioritize factors or somehow rank factors; Considering that the factors do not cover the same number of subjects; To control the statistical error, instead of entering the total score of the factors in the factor model, the average score of each factor was used, that is, when constructing the observable variable, the scores of the items in each factor

were added together and divided by the number of items. Then ranking was done based on T scores, presented in Table (3). According to the T values reported in this table, according to Shiraz Social Security Organization employees, among the 6 effective factors in the organization's cyber security, inefficient human resources, with a T value of 18.22, has taken the first rank. The second factor was the employee's position, with a T value of 17.06; the third factor was information protection culture with a T value of 14.29. The factors of capacity building, behavior and understanding of security, and budgeting and awareness are also assigned the fourth to sixth priority, respectively. Considering that the observed significance number is greater than 1.96, the significance of the obtained coefficients is confirmed with 95% confidence and an error of less than 5% ($P<0.05$). In addition, the correlation coefficients observed in the ranked factors also show the high convergent validity of these factors with each other ($P<0.01$).

As can be seen in the table, the strongest correlation coefficient was observed between "inefficient human resources and employee position" ($r=0.833$, $P<0.01$), and the weakest correlation coefficient was between "security behavior and perception" and "budgeting and awareness" ($r=0.212$, $P<0.01$).

5. Conclusion

Security in various social and economic dimensions is one of the most basic needs in human societies. The support collectively referred to as "social security" today is not new and belongs to the new era. Its origin can be related to the formation of the first human communities and civil societies and the formation and establishment of governments in societies. The roots of the emergence of social security in its modern and modern sense can be found in the industrial revolution and subsequent developments (from the middle of the 18^{th} century onwards). The developments after this event caused the creation of employment and solving problems, and improving the living standards of workers and the urban middle class, as a serious category for creating social security as a platform for increasing industrial production, to be considered by the leadership and management structure of different countries. After the Second World War, based on Article 22 of the Universal Declaration of Human Rights, social security was recognized as one of the basic human rights. According to the definition of the International Labor Organization, "Social security is the total support that society provides to its members in the face of economic and social distress caused by the interruption or reduction of income due to old age, disability, death, unemployment, illness, pregnancy, as well as compensation for medical and maintenance expenses. Gives." In today's modern societies, creating peace and hope for life and ensuring the access of members of the society to proper livelihood, welfare services, and needed social support; is considered one of the main duties of governments, but achieving these goals is not so easy. Any society's real and actual conditions are not such that all people have the same and completely fair minimum livelihood, peace of mind, and hope for the future. Even in the most advanced systems of income production and distribution, there are always people who, either due to lack of will and sufficient ability or due to reasons such as old age, disability, lack of supervision, mental and physical retardation, lack of work, or illness, are unable to meet related needs. By continuing to live, they do not have the means to earn a living and maintain their health.

The Social Security Organization of Iran is a public, non-governmental social insurance organization. This organization is responsible for the mandatory insurance coverage of workers, salary earners, and optional coverage of business owners and government and independent businesses. This organization is the first, oldest, and largest health and social security organization in Iran, which belongs to the insured. But this organization, like other big organizations in the country, will not be immune from cyberattacks. Considering that the Center for Political and International Studies of the country (2022) has also reported that we are currently witnessing a variety of cyberattacks; The social security organization, which is one of the important service organizations in the country, like other organizations, is at risk of cyberattacks. Therefore, it requires useful human resources to perform well in this field.

For this reason, cyber defense in this organization has been investigated by aiming to rank the factors affecting cyber security among the employees of the Social Security Organization of Shiraz City in 2023 so that we can identify the most important factors in line with that. According to the findings of the current research, according to the employees of the social security organization of Shiraz City, among the 6 effective factors in the cyber security of the organization are inefficient human resources; The position of the employee, and the culture of information protection are respectively the three most important factors affecting the cyber security of the Social Security Organization of Shiraz. Other factors are in the fourth to sixth categories.

Considering that expanding emerging and technology-based threats from adversaries and using cyberspace to conduct various operations towards land can cause a strategic surprise if do not consider it well [23], Also, due to the existence of valuable information related to insurance and people's health in the country's social security networks and the possibility of obtaining, vandalizing, disclosing and stealing this information, the need for cyber security to deal with such activities becomes more clear. In sum, different aspects of employees' lives are mixed with cyberspace, and any instability, insecurity, and challenges in this space directly affect different aspects of their lives, especially their security; therefore, awareness of cybersecurity is important. Considering that the awareness of this space is

related to culture and the approaches of organizations and institutions in the form of budgeting and capacity building to improve the behavior and understanding of the security of employees as well as empowering their human resources and turning them into efficient human resources will require huge costs. ; Therefore, to promote the culture of information protection that is related to the position of the employee in organizations, as well as reducing the costs related to empowering the human resources of organizations, paying attention to the 6 factors of budgeting and awareness, capacity building, security behavior and understanding, inefficient human resources, the position of the employee and the culture of information protection, and considering that among the 6 factors, the resources An inefficient human has taken the first rank, therefore, holding in-service courses to improve the level of employees' awareness of cyber security is one of the useful solutions that can be helpful and reduce possible time and financial costs for organizations.

Also, cyberspace has become an inseparable part of human life and has rapidly affected all areas of human life. Therefore, identifying the nature of this space and the conditions and requirements to become a capable actor in this field is the first step, and any inattention and neglect of this phenomenon will cause serious injuries and damage to society. They also considered that Iranian users are facing threats to privacy in cyberspace. Therefore, the most prominent security threats and damages in cyberspace are identity theft and fraud, spreading malware, theft, and misuse of information and personal data disclosure, unauthorized access to protected data, financial theft, electronic addiction, spreading rumors, creating suspicions, the tendency to commit crimes is the weakening of social norms and personal identity and other similar cases. Therefore, paying attention to things like inefficient human resources, The position of the employee, and the culture of information protection are recommended to the relevant authorities, and it is suggested to hold training classes to inform and empower the personnel in this area.

6. References

[1] A. Mardani., M. Eyouzi, "Investigating the impact of cyber security on the security and passive defense of the country", the first conference on passive defense and sustainable development, Tehran, 2016, [Online]. Available: https://sid.ir/paper/%20830874/fa [In Persian].

[2] F. Nouri, "Cyber space: hard security or soft security", 1th international conference on innovation and research in arts and humanities, Tehran, 2015, [Online]. Available: https://sid.ir/paper/823314/fa [In Persian].

[3] R. Malakouti., M. Khalilzadeh., "Legal Measure to Attain Cyber Security", Rasaneh, vol. 33, no. 1, pp. 69-97, 2022, [Online]. Available: https://sid.ir/paper/965214/fa [In Persian].

[4] N. Farzamnia., B. Abdi., A. Rezaiyan, "Presenting a Good Governance Model of Cyber Security in Defense Organizations", Military Management Quarterly, vol. 20, no. 77, pp. 81-120, 2020, [Online]. Available: https://sid.ir/paper/385775/fa [In Persian].

[5] Y. Beigzadeh., R. Ghasemi., Gh. Totunchi, "Cyber security in industrial control systems", 1th international research conference in science and technology, Tehran, 2015, [Online]. Available: https://sid.ir/paper/866831/fa [In Persian].

[6] S. Anusha., M. Nikjo., R. Kolivand, "Cyber security strategy", 3th national interdisciplinary research conference in engineering and management sciences, Tehran, 2021, [Online]. Available: https://sid.ir/paper/902054/fa [In Persian].

[7] "Information technology security news base", AFTANA, Online accesses 23. June 2022, News code: 19138. https://www.aftana.ir/news/19138/ایران-یازدهمین-مقصد-هکرها-جهان محبوب- [In Persian].

[8] A.B. Eghbali Zarch, "Center for Political and International Studies of the country", Online accesses 19. June 2022, " https://www.ipis.ir/portal/subjectview /684051/تهدیدات-و-حملات-سایبری-بر-علیه-ایران [In Persian].

[9] "Cyber security in Iran and the world", Online accesses 29. October 2022, https://www.nexterafactory.com/11831-2 /امنیت_سایبری [In Persian].

[10] A. Enaiati., Gh. Kordestani., A. Mohammadi Molgharni, "Provide a model for assessing financial sustainability in the Social Security Organization", Journal of accounting and social interests, vol. 12, no. 1, pp. 1-34, 2022, [Online]. Available: https://sid.ir/paper/1046359/fa [In Persian].

[11] Sh. Mashayekhi., M. Salehi., T. Enayati, "Review the gap between the existing and desired performance of the employees in order to implementation of the human performance improvement in the social security organization", Iranian Society for Training and Development, vol. 8, no. 29, pp. 123-141, 2021, [Online]. Available: https://sid.ir/paper/255530/fa [In Persian].

[12] "Portal of the Social Security Organization" https://tamin.ir/html/item/2554 [In Persian].

[13] A. Akhawan Tabasi., A. Amini Tarani., B. Tavakol, "Providing a conceptual model of professional competence of employees of large steel companies", Skill training quarterly. Vol. 6, no. 23, pp. 27-42, 2018, [Online]. Available: https://sid.ir/paper/409860/en.

[14] A. Behrad., M. Sabokrou., M. Tabatabaei nasab, "Designing Competency Model for the Head of Tax groups at Iranian National Tax Administration Based on Qualitative Approach", J Tax Res, vol. 26, no. 40, pp. 65-92, 2019, [Online]. Available: https://sid.ir/paper/375511/fa [In Persian].

[15] S. Ebrahimi., A. Pourreza., F. Farzianpour., A. Rahimi Foroushani, "Performance Assessment of Human Resource Management of the Social Security Organization Using the European Excellence Model (EFQM)", sjsph, vol. 15, no. 2, pp. 147-158, 2017, [Online]. Available: https://sid.ir/paper/84894/fa [In Persian].

[16] M. Ilkhani., H. Bahramzadeh, "Investigation of talent management and succession planning with organizational performance in the social security organization (case study of the General Administration of Social Security of North Khorasan province)", 2th national conference on management, psychology and behavioral sciences, Tehran,

2022, [Online]. Available: https://civilica.com/doc/1489791 [In Persian].
[17] R. Tat, "Investigation of factors affecting organizational performance from the perspective of organic structure; Inter-task coordination and tendency to learn (case study: Social Security Organization)", 1th national conference of applied studies in education and training processes, Bandar Abbas, 2021, [Online]. Available: https://civilica.com/doc/1293635 [In Persian].
[18] A. Sakhaei, "Meta-analysis of Satisfaction and Performance Evaluation of Social Security Organization", Social Security Journal, vol. 14, no. 3, pp. 55-90, 2018, [Online]. Available: Meta-analysis of Satisfaction and Performance Evaluation of Social Security Organization (ssor.ir).
[19] Z. Shirazian., R. Roustaei., Sh. Adelikhani., F. Jafari, "Study of the role of electronic monitoring on the performance evaluation of social security organization employees", 2th national accounting-management and economics conference with a sustainable employment approach and its role in the growth of the industry, Malayer, 2018, [Online]. Available: https://civilica.com/doc/844269 [In Persian].
[20] P. Malekinejad., S. Yousefi, "Effect of job satisfaction and administrative health on remote work goals, the mediating effect of protecting people's rights (case study: General Social Security Administration of Ilam province)", 2th Industrial engineering, management, accounting and economics conference, 2022, [Online]. Available: https://civilica.com/doc/1448487 [In Persian].
[21] A. Mahmoodabadi., M. Montazeri, "Investigating the impact of organizational justice on the voice of employees with the mediating role of organizational trust: a case study of the social security organization of Kerman province", the 4th international conference on knowledge and technology of the third millennium of Iran's economy, management and accounting, Tehran, 2021, [Online]. Available: https://civilica.com/doc/1236687 [In Persian].
[22] H. Doroshti., A. Fatemi Yeganeh, "The use of cyber tools in the information elite with an emphasis on the realm of security", Naja Strategic Studies Quarterly, vol. 5, no. 15, pp. 85-111, 2020, [Online]. Available: [Online]. Available: https://sid.ir/paper/387124/fa [In Persian].
[23] M. Mahdavipur., D. Azar, "I.R.I Army cybersecurity effective factors. (Case study: I.R.I Army general staff)", Military Science and Tactics, vol. 18, no. 60, pp. 103-123, 2022, [Online]. Available: https://civilica.com/doc/1607817 [In Persian].
[24] S. Heydari., M. Barzegar., A.H. Mohammad Davoodi, "Identify the Factors Affecting the Culture and Awareness of Cyber Security Using Theme Analysis", Electronic and Cyber Defense, vol. 11, no. 1, 67-80, 2023, [Online]. Available: magiran.com/p2594436 [In Persian].
[25] S. Heydari., M. Barzegar., A. Mohammad Davoudi, "Analyzing the Factor Structure of the Scale "Evaluation of Cyber Security Culture and Awareness" (Case study: Employees of Bank branches in Ahvaz City)", Psychological Methods and Models, vol. 14, no. 51, 113-126, 2023, [Online]. Available: magiran.com/p2593893 [In Persian].