August 2020

Designing and Psychometric Evaluation of Questionnaire of Human Factors Affecting Information Security in Libraries

Masoumeh Amini
Hamadan University of Medical Sciences, m.amini9274@gmail.com

Hossein VakiliMofrad
Hamadan University of Medical Sciences, vakili_hn@yahoo.com

Mohammad Karim Saberi
Hamadan University of Medical Sciences, mohamadsaberi@gmail.com

Designing and Psychometric Evaluation of Questionnaire of Human Factors Affecting Information Security in Libraries

Masoumeh Amini
MSc, Department of Medical Library and Information Sciences, School of Paramedicine, Hamadan University of Medical Sciences, Hamadan, Iran
E-mail: m.amini9274@gmail.com

Hossein VakiliMofrad
Assistant Professor, Department of Medical Library and Information Sciences, School of Paramedicine, Hamadan University of Medical Sciences, Hamadan, Iran
Corresponding Author: Vakili_hn@yahoo.com

Mohammad Karim Saberi
Assistant Professor, Department of Medical Library and Information Sciences, School of Paramedicine, Hamadan University of Medical Sciences, Hamadan, Iran
E-mail: mohamadsaberi@gmail.com

Abstract

Background and Purpose: Information security is the use of a set of policies, solutions, tools, hardware, and software to provide a threat-free environment in the generation, refinement, transmission, and distribution of information. The purpose of this study was to assess the validity and reliability of the Human Factors Inventory affecting libraries' information security.

Materials and methods: The present study was a cross-sectional study conducted for designing and psychometric evaluation for the inventory. After designing the initial list of inventory items, the opinion of expert lecturers and senior managers of Iranian libraries was used to evaluate face and content validity using Lawshe, content validity ratio (CVR) and Content validity index (CVI). Cronbach's alpha coefficient was used to assess the overall reliability of the questionnaire. Data were analyzed using SPSS software.

Results: The results showed that each of the items in the inventory had face validity and content validity (CVR> 0.75). Besides, the content validity index was set to 0.87 in all dimensions of the inventory, which is an acceptable number for the inventory. Cronbach's alpha coefficient was calculated as 0.946 and the reliability of the instrument was confirmed.

Originality/Value: In this study, for the first time, an inventory was designed and psychometrically assessed for human factors affecting library information security. Library and information science professionals and librarians can use this tool in research activities.

Keywords: Information security, inventory, validity, reliability, psychometric evaluation

Introduction

Information is one of the most important pillars in today's key decisions. No society achieves sustainable development except in the shadow of the intellectual maturity of its people; and intellectual maturity will not materialize unless through the proper generation, processing, maintenance and protection, and purposeful utilization of information (Ali Ahmadi, 2009). Provided that it is produced in a proper and purposeful manner and content, is exploited at the right time and in the right place, and most importantly, it is properly maintained and protected accurately and properly at all stages. In many organizations, the loss or damage of information can lead to irreparable damages and it might be very costly and difficult to recover it. As a result, the proper preservation and protection of information is one of the things that should be taken into consideration by the operators from the very beginning of its production(Khaleghi, 2004).

Organizations and their assets are today in a challenging environment. Among organizational assets, information is considered as an important and valuable asset for any organization; therefore, for protection and management of information and prevention of any misuse, it should be based on the most modern achievements and relevant standards(Almunawar, Susanto, & Tuan, 2011). To achieve this goal, each organization needs to design an information security management system depending on its level of information so that it can identify and manage the threats that the organization is exposed to. Therefore, organizations and companies need to implement security, which should be designed based on the needs of the organization and the importance of the information and can be a backbone for providing information capital(Soomro, Shah, & Ahmed, 2016). Thus, in the present day the most important asset of any individual or organization is information. Therefore, information security is one of the most important issues today(Eloff & Von Solms, 2000).

Information security means protecting information and information assets against any risks or threats. The risks and threats in this area include unauthorized access, use, disclosure, discontinuation, alteration, or destruction. Weakness in the information security dimension can have negative consequences for the organization and its information assets(Arianpour, Karbala Aghaei , & Abam, 2016). Information security is important because it protects information systems from internal and external threats. In fact, the fate of an organization depends on the levels of information technology and information protection of that organization(Jo, Kim, & Won, 2011).

Information systems security encompasses both technology and individuals (human factors) (Baghban Zadeh, 2014). Security always depends on people within the organization. In addition, as mentioned in the book ‘Information Security Guidelines’, many studies show that more than 80 percent of security problems in organizations are caused by inadvertent and deliberate errors by employees. Therefore, they emphasize that man is the most vulnerable element in the information security cycle, so paying attention to it helps us to achieve maximum security (Mahmoud Zadeh & Rad Rajabi, 2006).

Previous studies have shown that in addition to technological factors, human and organizational factors affect information security management (Hawkey et al., 2008). Also, the findings of most security research indicate that information security is primarily a human issue and equally an organizational or managerial issue (Wilson & Hash, 2003).

The diverse range of human factors can be summarized as follows: the science of recognizing the human characteristics and capabilities, ergonomics and the boundaries of human skills, and using this understanding to design, develop, and advance technology and services. In short, it refers to the interaction between human and computer. The link between people and technology reveals the fact that security weaknesses can easily occur depending on how people use technology or their perceptions of security (Khakbiz M, 2017).

Human factors also play an important role in computer security. Various factors such as individual differences, cognitive abilities, and personality traits can influence behavior. Information security behaviors are also strongly influenced by one's perception of risk. All of these factors are also influenced by the culture of the organization and the security environment. These factors interact and can lead to behaviors that are often detrimental to information security. Organizations must foster and maintain a culture in which positive security behaviors are valued, and the practical challenges associated with information security must be understood and addressed (Parsons.k, McCormac.A, Butavicius.M, & Ferguson, 2010).

Nowadays, the success of information security seems to be largely dependent on the effective behavior of those involved. Proper and constructive behaviors by users, system administrators, and other people can greatly enhance the effectiveness of information security, whereas malicious and destructive behaviors can substantially hinder its effectiveness. Human behavior (human factors) is complex and multi-faceted and this complexity challenges its control and predictability. The Organization for Economic Co-operation and Development (OECD) in its guidelines for information system security states: The diversity of system users, employees, consultants, customers, competitors, and overall the human factors and their varying levels of awareness, training, and interests have created potential problems for security (vali, Yaghoubi, & Oraee Yazdani, 2012).

As mentioned earlier, having robust security frameworks in an organization will never guarantee information security in the organization. Information security researchers and experts believe that humans are the weakest link in the security chain in organizations, so security breachers are thinking of infiltrating the chain through this link and taking over information systems. Nowadays, employees of the organizations with having such equipment as smartphones, tablets, and PCs that each have the ability to connect to organization’s networks, as well as their interest in presence in cyberspace and social networks, pose a serious threat to the security of any organization's information. In addition, organizations spend a great deal of money on security technologies and programs each year, but even with an uninformed employee on information security policies and programs, intruders will easily penetrate and infiltrate all security equipment and programs. This is why

most organizations focus on educating and informing their employees to maintain information capital(Bishop, 2005).

With the advent of modern technologies in libraries and information centers, attention has been given to the data and information available in libraries and information centers and their presentation to clients, and libraries and information centers as an organization for storing and retrieving information needed users play an important role in meeting their information needs. In the meantime, libraries and academic information centers, due to the particular type of client, need to provide specific types of resources and databases that providing this specialized information in turn lead to developing personal knowledge, increasing the level of knowledge and awareness of the academic community, expanding the sciences and research etc. Libraries and public information centers also offer a variety of information resources and services due to the wide range of users of varying ages and information needs, and since the enormous costs are spent in procuring and purchasing resources and databases in libraries and academic and public information centers, the protection and security of information becomes more urgent.

Considering the importance of information security in libraries and information centers, ‹ (Peltier, 2016) argues that library information systems provide online services to intra-organizational and inter-organization customers, which makes security risks for these systems due to accessing these systems through internet. Websites are now one of the most important tools for accessing libraries and gateways to guide users to information resources. Therefore, there is a need for security in the design and implementation of library websites (Habibi, Seyed-Akbari, Torab-Miandoab, & Samad-Soltani, 2019).

Thus, with regard to the key role of human factors in information security of libraries and information centers, the present study designed and psychometrically evaluated the inventory of human factors affecting information security in libraries, and attempted to design and develop a standard model and questionnaire in this regard and suggest solutions to to implement information security enhancements for managers, policymakers, librarians and informants in order to improve security effectiveness in libraries and promote the level of information security in libraries and to provide better services.

Conceptual Model of Research

Investigating relevant studies in the field of information security and using human factors as stated in previous studies, the conceptual model of research as the model of human factors affecting information security is presented as follows:

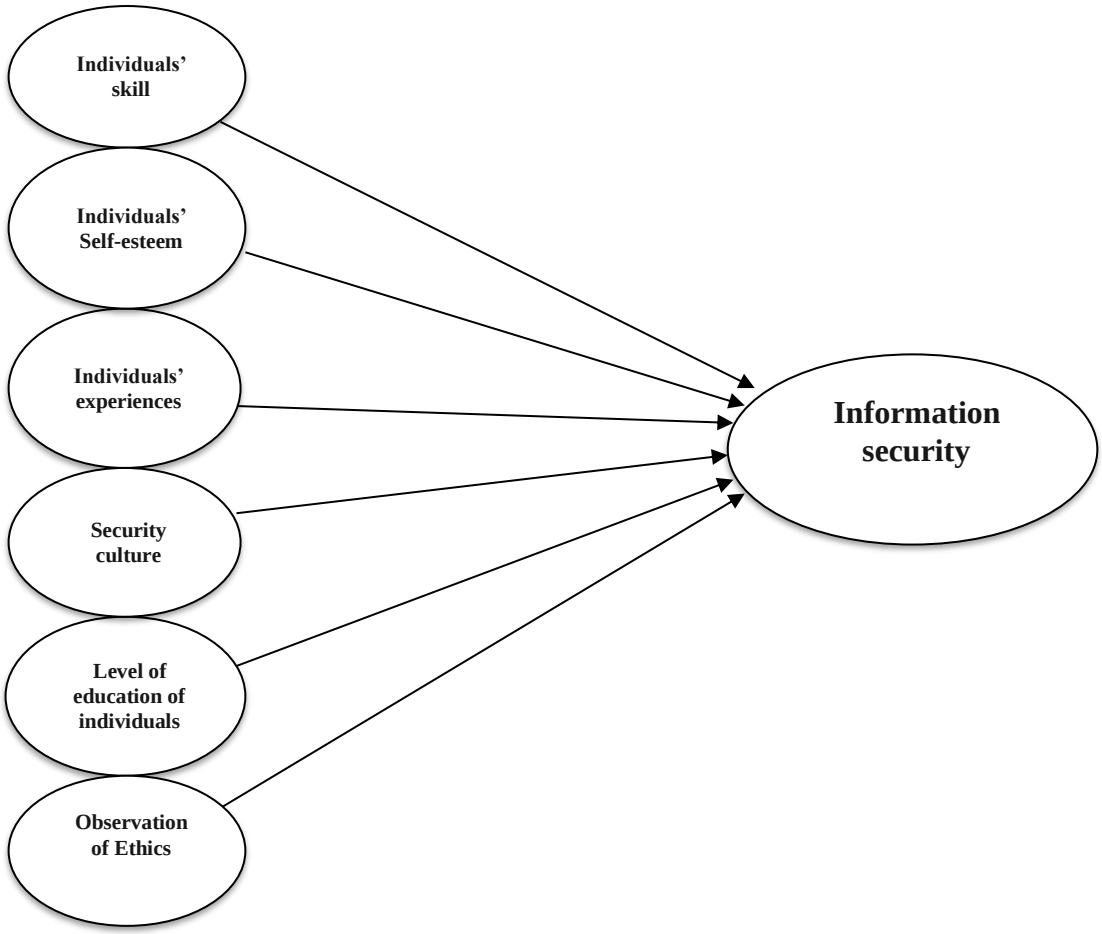

Figure 1. Model of Human Factors Affecting Information Security

As shown in Figure 1, the conceptual model of the research was designed in the form of 6 main variables. Variable of individuals' skill and experiences was derived from conceptual model of Alavi (Alavi, Islam, & Lee, 2016), variable of security culture and individuals' self-esteem was derived from conceptual model of Taheri (Taheri, 2007), variable of Individuals' level of education was derived from conceptual model of Kaviani (Kaviani, Tajfar, & Karimzadegan Moghadam, 2013) , and variable of Observation of Ethics was derived from conceptual model of Baghban Zadeh (Baghban Zadeh, 2014) . Finally, based on the above model, human factors affecting information security in libraries and information centers were evaluated. Therefore, the basic constructs that are examined in this research are: 1. Individuals' Skills 2. Individuals' Experiences 3. Security Culture 4. Individuals' Self-esteem 5. Education level of Individuals 6. Observation of Ethics. The following is a brief description of each of the above constructs.

1. Individuals' Skill

Skills play an important role in human performance. Education is also important in developing skills, and demonstrating a commitment to maintaining professional competence and skills is one of the key forces in dealing with information science issues, which in the absence of adequate and appropriate skills in staffs leads to their poor performance.

Therefore, staff need to have sufficient skills to meet the requirements of information security policy (Alavi et al., 2016).

2. Individuals' Experiences

Individuals with sufficient experience and adequate computer capabilities, and expertise in information security related activities will be more successful in conducting assigned tasks and making decisions related to the organizational goals. Hence, having the individuals' skills and experience is one of the most effective human factors in information security.

3. Security Culture

Having a positive attitude throughout the organization about information systems security activities and supporting organizational values of security activities makes security culture one of the most effective human factors in information security. In the information systems literature, organizational culture has been studied as a powerful force against new technologies and developments and as a means of accepting information technology and as a factor influencing organizational security.

4. Individuals' Self-esteem

With the awareness of the importance and necessity of compliance with laws and regulations and the proper implementation of security activities, individuals can move forward to meet the organization's security goals. Employee commitment and loyalty to the organization and maintaining information security are also factors that make self-esteem an influential human factor in information security (Baghban Zadeh, 2014).

5. Individuals' Level of Education

One of the effective human factors in providing information security is awareness and information security training of users. Also, one of the best ways to reduce security risks in organizations is to keep employees aware of security issues, which means that they must take responsibility for their actions in the workplace (Kaviani et al., 2013).

6. Observation of Ethics

Taking social responsibility for an organization encompasses the principles of professional ethics. From the human point of view, the use of control and security means can have a detrimental or beneficial effect on staff behavior and may lead to some resistance, leading people to depart from ethical standards. Human force committed to work ethics and organizational values is not only a factor for an organization's superiority over the other, but also a sustainable competitive advantage for many organizations. Ronaghy and Feizi in their research entitled 'Work ethic and its relationship with information security management' acknowledge that information security management has a positive and significant relationship with employees' work ethic, meaning that using information security tools and

implementing strategies and measures in this area, not only did not have a negative impact on work ethic compliance, but the results also showed a positive interaction with ethical standards (Baghban Zadeh, 2014).

Methodology

This study is a cross-sectional study. The purpose of this study was to assess the validity and reliability of the Human Factors Affecting Inventory of Libraries Information Security. In order to determine the content validity ratio and index, 8 experts and senior managers of Iranian libraries were selected and asked to comment on the appropriateness of each questionnaire. Three criteria of "relevance", "clarity", "simplicity" was used to determine the face validity of the inventory.

The four-point Likert scale for "simplicity" included: 1. The phrase is incomprehensible. 2. The phrase needs to change a lot. 3. The phrase needs little change. 4. The phrase is quite comprehensible.

The four-point Likert scale for criterion of "relevance" included: 1. The phrase is irrelevant. 2. The phrase needs to change a lot. 3. The phrase needs little change. 4. The phrase is quite relevant.

The four-point Likert scale for criterion of "clarity" included: 1. The phrase is vague. 2. The phrase needs to change a lot. 3. The phrase needs little change. 4. The phrase is clear.

After designing the inventory and distributing it to library professionals and managers, the CVI was first calculated for each criterion, and then averaged, and items with a CVI above 0.79 were accepted and items with a CVI less than 0.79% were modified and revised. Finally, the content validity index for each item is calculated using Formula 1.

$$\text{Content Validity Index} = \frac{\text{The number of the experts who have assigned score 3 or 4 to the item}}{\text{The total number of experts}}$$

Formula 1. Calculation of content validity index of questionnaire items

To determine the validity coefficient, three criteria of "necessary", "useful" and "unnecessary" were used. Finally, the content validity ratio for each item is calculated using Formula 2.

$$\text{Content Validity Ratio} = \frac{\text{The number of necessary responses in each item} - \frac{\text{the total number of participants}}{2}}{\frac{\text{The total number of participants}}{2}}$$

Formula 2. Calculation of the content validity ratio of the questionnaire items

It should be noted that the acceptance or rejection of the questionnaire was done according to the following criteria: 1. If the CVR value of the item is equal to or greater than 0.75 the item will be accepted. 2. If the CVR value of the item is between zero and 0.75 and its impact score is greater than 2, the item will be accepted. 3. If the CVR value of the item is less than zero and its impact score is less than 2, the item will be rejected. The impact score (the numerical mean of judgments) indicates the number of opinions of experts who agree with the necessity of an item. Finally, the impact score for each item is calculated using Formula 3.

$$\text{Impact score} = \frac{\text{Sum of the frequency repetition of score by the target group}}{\text{The number of member in the target group}}$$

Formula 3. Calculation of the impact score of questionnaire items

Given that the number of specialists involved in the present study was 8, CVR values above 0.75 were accepted according to Table 1.

Table 1: Minimum acceptable CVR values for different number of specialists (Lawshe, 1975)

The number of experts (participants)	The minimum value of content validity ratio
5	0.99
6	0.99
7	0.99
8	0.75
9	0.78
10	0.62
11	0.59
12	0.56

Results

At the beginning of the study, the initial questionnaire had 45 items. After assessing face and content validity, 5 items were deleted due to lower CVR (0.75) and 12 items due to CVI less than 0.79, were reviewed and edited. Finally, the final version of the questionnaire was approved with 40 items. Following, according to Table 2, the values of CVR, CVI, impact

score (numerical mean of judgments) and results of acceptance or rejection of each item are presented.

Table 2. CVR. CVI values of impact score, results of acceptance or rejection of each item

No.	item	CVR	CVI	Impact score	acceptance or rejection of item
Information security					
1	The information security policy document is prepared in the library by the management and will announced to all staff after publication.	0.25	0.10	2.375	Acceptance
2	The information security structure of the library has been developed in line with the policy.	0.25	0.10	2.5	Acceptance
3	Library planning is designed to improve information security.	0.50	0.83	2.625	Acceptance
4	The technical and management standards are implemented in library to improve information security.	0.25	0.75	2.625	Acceptance
5	There exists integrated software in library for promoting information security.	0.25	0.83	2.625	Acceptance
6	Information security monitoring systems record daily, weekly and monthly reports in libraries.	0	0.66	2.375	Acceptance
7	A back-up is used in library for protecting information security.	0.25	0.10	2.625	Acceptance
8	The architecture of building and arrangement of library sections are designed in such way that information security is preserved.	-0.25	0.87	2.25	Rejection
9	The security of all information sources, including digital resources and databases in library is observed.	0.25	0.75	2.625	Acceptance
10	Security rules are implemented in all sections of library (Loan Section / Reference Section / Technical Services).	0.25	0.91	2.625	Acceptance
11	Valuable information resources are encrypted in the library.	0.50	0.70	2.625	Acceptance
12	There is legal acceptance of information security in libraries.	0.75	0.70	2.875	Acceptance
13	Observing the ethics and privacy of individuals is important in library.	0.75	0.87	2.75	Acceptance
14	It is important to have a customer relationship management in the area of information security in library.	0.25	0.91	2.5	Acceptance
15	An effective and appropriate management action is taken by the library against security breaches.	0.25	0.75	2.625	Acceptance
human factors affecting information security					
1	To what extent do you find it necessary to use a variety of educational tools to teach information security related activities in the library?	0.75	0.87	3.125	Acceptance
2	To what extent have you participated in training programs on library security and related information systems?	0.75	0.87	2.75	Acceptance

3	How effective has the organization's training courses been on your awareness of library security issues and threats?	-0.25	0.62	2	Rejection
4	To what extent is in-service training necessary to enhance information security in libraries?	0.25	0.87	2.625	Acceptance
5	How much do you agree "administrators, librarians, staff, and users should have the same level of education on library security issues"?	0.50	0.83	2.75	Acceptance
6	How would you rate your direct experience in information security in libraries?	0.25	0.79	2.375	Acceptance
7	How do you evaluate your indirect experience in preserving and interpreting relevant information in the library and in preserving existing software and hardware?	0.75	0.79	2.875	Acceptance
8	How much do you agree with the idea that "experiences of non-expert individuals on security issues should not be used"?	0.25	0.87	2.25	Acceptance
9	To what extent your experience and opinions on security issues have been used in your place of employment.	-0.25	0.75	2	Rejection
10	How much do you agree with the idea that "good experiences of staffs on security issues should be used in libraries"?	0.50	0.87	2.625	Acceptance
11	How important is the availability of computer skills and expertise in library security related activities?	0.75	0.87	2.75	Acceptance
12	How do you evaluate your ability to deal with security issues in libraries?	0.25	0.75	2.375	Acceptance
13	To what extent do employees need to be skilled in dealing with security issues?	0.75	0.87	2.875	Acceptance
14	What level do librarians have in dealing with security issues?	-0.25	0.70	2	Rejection
15	What level of proficiency and skill should a library manager have in managing information security?	0.25	0.75	2.5	Acceptance
16	How important is a positive attitude throughout the library organization towards information security activities?	0.50	0.87	2.75	Acceptance
17	How essential is an information security culture among librarians and library staff?	0	0.87	2.5	Acceptance
18	To what extent is it necessary for the library's organizational values to support information security activities?	0.75	0.87	2.875	Acceptance
19	How much information security culture does your library have?	0.25	0.79	2.5	Acceptance
20	To what extent do librarians and staff welcome the creation of an information security culture in the library?	0.25	0.75	2.375	Acceptance
21	To what extent is it necessary for managers and librarians to understand the importance and necessity of following laws and implementing security activities?	0.25	0.79	2.5	Acceptance
22	To what extent is the commitment and loyalty of library staff necessary for the organization and maintenance of information security?	0.75	0.87	2.875	Acceptance
23	To what extent is it necessary for managers and librarians to participate in maintaining	0.25	0.87	2.5	Acceptance

	information security?				
24	To what extent do librarians and staff feel they have a good understanding of information security and how to deal with security issues in the library?	0	0.87	2.375	Acceptance
25	How effective are staff preparedness and self-esteem to answer users' questions about library security issues?	0.25	0.70	2.25	Acceptance
26	To what extent is it necessary to adhere to library security policies (protecting library organization information and technology from security breaches)?	0.50	0.87	2.625	Acceptance
27	How important is the existence of an integrated management system in libraries?	0.25	0.66	2.375	Acceptance
28	To what extent is it necessary to punish offending personnel for not maintaining information security in the library?	0.25	0.75	2.375	Acceptance
29	To what extent are you committed to maintaining and adhering to the security rules in your library?	0.50	0.79	2.625	Acceptance
30	To what extent do you consider the use of security and control systems effective in employee behavior?	-0.25	0.87	2.125	Rejection

Content validity index (CVI), which represents the completeness of the judgments regarding the validity or applicability of the final questionnaire, was calculated as 0.87 using the CVI formula. Therefore, this questionnaire was designed with an acceptable level of content validity index. The reliability of the questionnaire was calculated using Cronbach's alpha coefficient, which can be a number between zero and one, and was 0.946. Table 3 shows the Cronbach's alpha coefficient values for each of the variables.

Table 3. Cronbach's alpha coefficient for information security and effective factors

No.	Variable	Number of Items	Cronbach's alpha coefficient	Cronbach's alpha for the total items
1	Information security	14	0.871	0.946
2	Education level	4	0.795	
3	Experiences	4	0.815	
4	Skill level	4	0.794	
5	Security culture	5	0.850	
6	self-esteem	5	0.755	
7	Ethics	4	0.727	

Discussion and Conclusion

(Nkiki & Yusuf, 2008) believe that information is an essential part of a nation's resources and that access to it is a fundamental human right. Information is not only a national source but also a means of social communication.

As there is extensive and varied information in the library collection, Libraries need to be safe from security threats and vulnerabilities. Therefore, resource management faces challenges that require the necessary skills to cope. One of the challenges in libraries is the issue of collection security for print and non-print sources. Thus, for the safety of the collection, it is important that the staff and users have awareness and they must be aware of the importance of securing their library collection. Lack of awareness may result in deliberate or unwanted breach of security of the collection. Hence, libraries should be designed in a way that ensures collection security, collection security issues should not be assigned to an employee's judgment, and policies and procedures must be precisely established and implemented. Such policies should be sent and communicated to staff and users (Atiku Maidabino & Awang Ngah, 2010). (Udoumoh & Okoro, 2007) also believe that libraries develop policies to ensure the efficient use of library resources.

Libraries and information centers are one of the important centers in accessing the information needed and play an important role in meeting the information needs of different segments of society including educational and research information. Thus, providing, protecting, and accessing this high volume of information in such organizations costs a great deal, and it is natural that to protect their information, especially databases or any electronic and digital resources, etc. they should have more effort and accuracy. Therefore, it is necessary for these organizations to develop guidelines for implementing information security practices.

As a result, information security is a critical issue in all organizations, and the success of information security in all organizations, including libraries and information centers, largely depends on the effective behavior of librarians, managers, users, and all of the human factors in that organization. Thus, it is essential that human factors affecting information security be accurately identified so that they can be used to fulfill security objectives in libraries and information centers.

(Baghban Zadeh, 2014) in a study, entitled "Identifying and Prioritizing Human Factors Affecting Information Security" examined this subject. In this regard, at first using the research literature and research on the subject of research, the basic indexes were identified and based on the proposed research model, 27 indexes were identified and grouped in nine dimensions of top management support, security culture, security education, security policy, direct experiences, self-esteem, skill, ethics, and security behavior. (EllahI, Taheri, & Hasanzadeh, 2008) Conducted a study entitled "Providing a Framework for Human Factors Related to Security of Information Systems". Constructs of "Top management support, security training, security culture, security skills, security policy enhancement, experiences, and self-confidence" were identified as effective factors on the effectiveness of information systems security. Also in a study entitled "Library and Information Security: Official and Electronic Security Measures» by (Ferdinand, Patrick, & Thelma, 2015) , they concluded that since the nature and usefulness of the telecommunications security and communications system in libraries help to provide maximum security for library staff, resources and equipment and the entire library complex, it is essential that these telecommunications

systems and devices are available in the library. However, the use of security system and telecommunications and management systems, staff support, software development, hardware upgrades, and achieving set goals requires funding.(Kruger, Drevin, & Steyn, 2010) A study entitled "Assessment of Information Security Awareness through Testing User Knowledge and Behavior" was conducted. The purpose of this paper was to report on the development of a prototype model for measuring information security awareness at the International Mining Company. The method used to develop measuring instruments was based on techniques taken from social psychology, which suggests that these demands for responding favorably or unfavorably to a particular object have three components: Impact, behavior and cognition. The component of impact includes one's positive and negative feelings about something. The component of behavior involves the intention to act in certain ways, whereas the component of cognition refers to the beliefs and thoughts of an object. Finally, they concluded that the level of knowledge of employees about information security is moderate and needs more training and attention, and in order to raise the level of awareness of information security, it is necessary to put more effort in each domain of knowledge and attitude. (Shaw, Charlie, Harris, & Huang, 2009) A study entitled "Investigating the Evaluation of Information Richness on Users' Information Security Awareness in the Online Environment". They divided the information security awareness into three levels of reception, perception and output, and expressed the information richness in online education based on hypertext, multimedia, and hypermedia. Therefore, these studies have restricted themselves to some areas of information security or assessed the status of research activities from the perspective of information security management. Therefore, by reviewing related research, it can be concluded that no study has been conducted so far on designing and psychometric evaluation of human factors affecting information security in libraries. Thus, given the confirmation of face and content validity, the present study could be useful to researchers, including librarians and information scientists and librarians, in similar communities, especially in libraries and academic and public information centers.

With these interpretations, the purpose of the present study was to design and psychometric evaluation the human factors questionnaire affecting information security of libraries. Considering the CVR values and the impact score (numerical mean of judgments), 40 items were accepted. In this study, content validity index (CVI) and coefficient of validity ratio (CVR) were calculated to evaluate the content validity of the questionnaire. Therefore, based on the obtained values, the questionnaire for identifying human factors affecting information security has adequate face and content validity and its face and content validity confirms the relevance, clarity and simplicity of items. In addition, the Cronbach's alpha coefficient in the designed questionnaire indicates high internal consistency of the expressions and confirms the reliability of the tool.

The main significance of this study was that its tool was designed based on the human factors affecting information security in six components: Individuals' Skill, Individuals' Experiences, Security Culture, Individuals' Self-esteem, Individuals' Level of Education, Observation of Ethics and in fact achieving this model provided the questionnaire requested.

Although this model (Human Factors Affecting Information Security) does not cover all the important aspects, it nevertheless focuses on areas using which effective information security programs can be designed and developed for security of libraries and information centers, and they can be used to achieve security goals. Therefore, it seems useful to use this tool in academic and public libraries and information centers. It should be noted that the present tool provides opportunities for senior managers and planners of libraries and information centers to identify and apply human factors affecting information security, improve security effectiveness for their libraries and information centers, as well as strengthen their strengths and address existing weaknesses to move toward their organization's goals, i.e., delivering desirable services and meeting the diverse information needs of the community.

As a result, to address all the weaknesses in libraries and academic and public information centers, library managers and administrators are suggested to utilize similar questionnaires to design and psychometrically evaluate questionnaires appropriate to the type and structure of the organization as well as to design related models. They use all their abilities to solve problems by planning and taking appropriate actions, and train human forces on security issues by planning and such measures as allocating part of the budget to advance security objectives, conducting classes and training courses on familiarity with information security issues and the use of varied and up-to-date training tools. Also, by increasing the level of knowledge of librarians and information security professionals on information security, enhancing their security skills and experiences, increasing their motivation and self-confidence, working to create, improve and enhance an appropriate security culture in libraries and information centers, as well as by observing ethical standards on all security issues it is possible to reduce human errors in information security and bring about a desirable level of information security in libraries and information centers in terms of human resources. Therefore, due to the high importance of information security in providing better services and promoting the level of information security in libraries and information centers, this questionnaire was designed and evaluated and it is worth mentioning that the questionnaire is easy to use and researchers can use it in their research activities.

Acknowledgement

This research is part of a Master's thesis in Librarianship and Medical Information Science approved by code 980217866 at Hamedan University of Medical Sciences (Iran). The authors would like to acknowledge and thank the librarians and informants of Hamedan University of Medical Sciences for their contribution to this research.

References

Alavi, R., Islam, S., & Lee, W. C. (2016). A Risk-Driven Investment Model for Analysing Human Factors in Information Security. (A thesis submitted for the degree of Doctor

of Philosophy), The University of East London, School of Architecture, Computing and Engineering (ACE).

Ali Ahmadi, A. (2009). ICT Strategic Planning. Tehran: Knowledge Production Publications, [Persian].

Almunawar, M., Susanto, H., & Tuan, y. (2011). “information security management system standards: Acomparitive study of the big five". Inter-national journal of electrical & computer sciences IJECS-IJENS, 11, 23-27.

Arianpour, M., Karbala Aghaei , K., & Abam, Z. (2016). Compliance with ISO / IAS Standards. 27002 and 27019 in the field of "Information Security Management" at the National Library and Archives of the Islamic Republic of Iran. (Arshad thesis), Alzahra University, Faculty of Educational Sciences and Psychology, Department of Information Science and Dentistry. [Persian].

Atiku Maidabino, A., & Awang Ngah, Z. (2010). Collection Security Issues in Malaysian Academic Libraries: An Exploratory Survey. Library Philosophy and Practice.

Baghban Zadeh, M. (2014). Identification and validation of human factors affecting information security using the ANP and DEMATEL combined fuzzy approach. (Master's thesis).[Persian]).

Bishop, M. (2005). Position: Insider is relative. In: C.F. Hempelmann and V. Raskin (eds.), Proceedings of the New Security Paradigms Workshop. New York: ACM Press.

EllahI, S., Taheri, M., & Hasanzadeh, A. (2008). A framework for human-related factors in information system security. Management researches in Iran., 13(2), 1-22. [Persian].

Eloff, M. M., & Von Solms, S. H. (2000). Information security management: anapproach to combine process certification and productevaluation. Computers & Security, 19(8), 698–709.

Ferdinand, O., Patrick, I., & Thelma, N. (2015). library and information resources security: traditional and electronic security measures. International journal of academic research and reflection, 3(3).

Habibi, S. H., Seyed-Akbari, L., Torab-Miandoab, A., & Samad-Soltani, T. (2019). Usability of Central Library Websites of Iranian Universities of Medical Sciences: An Evaluation. Desidoc Journal of Library & Information Technology, 39(4), 162-168. doi:10.14429/djlit.39.4.14462. [Persian]

Hawkey, K., Botta, D., Werlinger, R., Muldner, K., Gagne, A., & Beznosov, K. (2008). Human, Organizational, and Technological Factors of IT Security. In CHI’08 extended abstract on Human factors in computing systems. 3639–3644.

Jo, H., Kim, S., & Won, D. (2011). Advanced information security management evaluation system. KSII T Internet Info. 5(6).

Kaviani, M., Tajfar, A. H., & Karimzadegan Moghadam, D. (2013). Presenting a framework for identifying effective factors on end users awareness and its role on computer information security in Banks- Case study: Bank Melli. (A Thesis Submitted for the Award of Master of Science Degree management Information security.[Persian]).

Khakbiz M, M. S. A., Mirghafori H. (2017). Identification and Prioritization Of Organizational Information Systems Security Factors Using MADM: Yazd University Faculty of Economics, Management & Accounting Thesis submitted for master degree of Industrial management.[Persian].

Khaleghi, M. (2004). Implementation guide for information security management system. Tehran: Secretariat of the Supreme Council for the Security of the Information Interchange Space. [Persian].

Kruger, H. A., Drevin, L., & Steyn, T. (2010). A Vocabulary test to assess information. Information Management & Computer Security Journal. 18(5), 316-319.

Lawshe, C. (1975). A Qualitative Approach to Content Validity. Personnel Psychology 28(8), 563-575.

Mahmoud Zadeh, I., & Rad Rajabi, M. (2006). Security management in information systems. Journal of Management Sciences of Iran, 1(4), 78-112. [Persian].

Nkiki, C., & Yusuf, F. O. (2008). Library and information support for New Partnership for Africa's Development (NEPAD). Library Philosophy and Practices.

Parsons.k, McCormac.A, Butavicius.M, & Ferguson, L. (2010). Human Factors and Information Security: Individual, Culture and Security Environment. Defence science and Technology Organisation. Command, Control, Communications and Intelligence Division.

Peltier, T. R. (2016). Information Security Policies, Procedures, and Standards: Guidelines for effective information security management. CRC Press.

Shaw, R. S., Charlie, C., Harris, A., & Huang, H. j. (2009). The impact of information richness on information security awareness training effectiveness. Computer & Education(52), 93-100.

Soomro, Z., Shah, M., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), 215-225. doi:10.1016.

Taheri, M. (2007). Providing a framework for the role of human factors in the security of information systems. (Master thesis), Tehran: Tarbiat Modarres University- Faculty of Humanities- Department of Information Technology Management.[Persian].

Udoumoh, C. N., & Okoro, C. C. (2007). The effect of library policies on overdue materials in university libraries in the South-South Zone, Nigeria. Library Philosophy and Practice.

vali, H., Yaghoubi, N., & Oraee Yazdani, B. (2012). Identifying and prioritizing the factors affecting the adoption and development of information security policies in the organization (Study at the National Iranian Oil Products Distribution Company). (Master's thesis. [Persian]).

Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. National Institute of Standards and Technology, 20-79.

Appendix 1: Final version of the Human Factors Inventory Affecting of Information Security in Libraries Questionnaire

No.	Item	Totally disagree	disagree	No idea	agree	Totally agree
Information security						
1	The information security policy document is prepared in the library by the management and will announced to all staff after publication.					
2	The information security structure of the library has been developed in line with the policy.					
3	Library planning is designed to improve information security.					
4	The technical and management standards are implemented in library to improve information security.					
5	There exists integrated software in library for promoting information security.					
6	Information security monitoring systems record daily, weekly and monthly reports in libraries.					
7	A back-up is used in library for protecting information security.					
8	The security of all information sources, including digital resources and databases in library is observed.					
9	Security rules are implemented in all sections of library (Loan Section / Reference Section / Technical Services).					
10	Valuable information resources are encrypted in the library.					

11	There is legal acceptance of information security in libraries.					
12	Observing the ethics and privacy of individuals is important in library.					
13	It is important to have a customer relationship management in the area of information security in library.					
14	An effective and appropriate management action is taken by the library against security breaches.					
No.	**Item**	**Very low**	**Low**	**Average**	**High**	**Very high**
human factors affecting information security						
1	To what extent do you find it necessary to use a variety of educational tools to teach information security related activities in the library?					
2	To what extent have you participated in training programs on library security and related information systems?					
3	To what extent is in-service training necessary to enhance information security in libraries?					
4	How much do you agree "administrators, librarians, staff, and users should have the same level of education on library security issues"?					
5	How would you rate your direct experience in information security in libraries?					
6	How do you evaluate your indirect experience in preserving and interpreting relevant information in the library and in preserving existing software and hardware?					
7	How much do you agree with the idea that "experiences of non-expert individuals on security issues should not be used"?					
8	How much do you agree with the idea that "good experiences of staffs on security issues should be used in libraries"?					
9	How important is the availability of computer skills and expertise in library security related activities?					
10	How do you evaluate your ability to deal with security issues in libraries?					
11	To what extent do employees need to be skilled in dealing with security issues?					
12	What level of proficiency and skill should a library manager have in managing information security?					
13	How important is the availability of computer skills and expertise in library security related activities?					
14	How essential is an information security					

	culture among librarians and library staff?					
15	To what extent is it necessary for the library's organizational values to support information security activities?					
16	How much information security culture does your library have?					
17	To what extent do librarians and staff welcome the creation of an information security culture in the library?					
18	To what extent is it necessary for managers and librarians to understand the importance and necessity of following laws and implementing security activities?					
19	To what extent is the commitment and loyalty of library staff necessary for the organization and maintenance of information security?					
20	To what extent is it necessary for managers and librarians to participate in maintaining information security?					
21	To what extent do librarians and staff feel they have a good understanding of information security and how to deal with security issues in the library?					
22	How effective are staff preparedness and self-esteem to answer users' questions about library security issues?					
23	To what extent is it necessary to adhere to library security policies (protecting library organization information and technology from security breaches)?					
24	How important is the existence of an integrated management system in libraries?					
25	To what extent is it necessary to punish offending personnel for not maintaining information security in the library?					
26	To what extent are you committed to maintaining and adhering to the security rules in your library?					