International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: SJIF: 5.995
Available Online at www.journalijcar.org
Volume 6; Issue 11; November 2017; Page No. 7247-7252
DOI: http://dx.doi.org/10.24327/ijcar.2017.7252.1109

Research Article

ASPECTS OF HUMAN FACTOR FOR INFORMATION SECURITY MANAGEMENT IN ACADEMIC LIBRARIES

Shivarama J* and Vaishali A. Dawar

Centre for Library and Information Management Studies, Tata Institute of Social Sciences, Deonar, Mumbai

A R T I C L E I N F O

Article History:

Received 18th August, 2017
Received in revised form 13th September, 2017
Accepted 30th October, 2017
Published online 28th November, 2017

Key words:

Human factors, information security management, university libraries, Digital information security, human aspects in information security

A B S T R A C T

In the digital world security of digital information assets of university libraries have become very essential. Looking at the precipitous information security breaches at almost all aspects of life and considering the research work taking place in universities and supported by the libraries, the problem of information security in university libraries is becoming bigger and dangerous. Each step of information beginning from collection, processing to dissemination involves security, which involves technical, management and social challenges for the libraries. Information system security depends upon humans using the system and their behavior within the system environment. Hence human factors require adequate attention as they are the main causes for incidents in information security.

This article gives an overview of the human factors with regards to information security in university libraries, with a holistic approach to human factors. Further it provides ways to classify these factors in different categories and compare them with information security management standard 27001. This article will be useful for research studies involving human factors in information security management in university libraries, and also for other research in management or library and information science, where human factors are involved.

INTRODUCTION

From the past evidences of university library website hacking, website defamation, ransomeware attack, etc. it is evident that any institution is vulnerable to various kinds of technological jargons or technical threats while using information and communication technology. For a university library starting from collection, storage, process and dissemination, every step needs ICT applications and hence information security is required at each step. Information assets in University Library are important for academic development of students, for research requirements of researchers and for teaching-learning process for faculties. The university library needs to protect its digital assets in terms of website, web portal, repository, metadata, library software and its data, personal information of each student, faculties and staff members, and such other digital resources in the library's possession. The data about researches and their research work is very sensitive and susceptible to theft or destruction or any kind of misuse. The problem with information security is because the attack can be noticed only after it is attempted and detected. Hence information security represents a significant technical, management and social challenges for the libraries, which require investing in the human factor besides technical factors as necessity because technology is ultimately used by people. Both human and technological elements are indispensable for effective practices of information security management system and both cannot be considered separately.

Information security is not solely a technical factor; it depends upon humans using the system and their behavior within the system environment and thus human factors require adequate attention as they are the main causes for incidents in information security.

The reasons for requirement of information security in university libraries are:

- Information security is a practice of preventing anybody's unauthorized access to our own digital property, as the unknown person may use it for illegal purpose, disclose, disrupt, modify, inspect, delete, record, copy or destruct the digital information from anywhere and at any time through various networks, especially Internet.
- The online digital information assets of any person or institution are continuously exposed to attention of cybercriminals. The threats may be in the form of hacking, inserting viruses or worms in the system, data loss, server damage, stopping of user services,

Corresponding author:* **Shivarama J
Centre for Library and Information Management Studies, Tata Institute of Social Sciences, Deonar, Mumbai

denied access to website and portal, publishing illegal and unethical contents and many more.

- The impact of information security incidences on organization can be loss of confidentiality, injuries to availability, critical data exposure, services vandalism, loss of reliability and trust, economic loses, etc.
- The intruder illegally accessing and using our data may not cost much, but the organization may need to face huge losses in terms of finances, trust and legal actions.

Objectives

The two major factors of information security management are technological factors and human factors. This article considers only human factors. The human factor in information security is the most important factor because it is the root cause of all problems. This paper tries to take an overview of all the aspects associated with human factor with regard to information security in university libraries. The human can be either a protector or an intruder who is trying an unauthentic access to information owned by others. Hence the objectives of this paper are:

1. To trace the human factors associated with information security in university libraries viewed from two approaches
   a. human factor aspects- organizational
   b. human factor aspects- individual
2. To find the human aspects in compliance with the information security management standard ISO/ISE 27001.
3. To find the ways of classification for aspects of human factor.

Conceptual framework

Information Security management is a process of defining the security controls in order to protect the information assets (E-Government Act of 2002). The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed (ISO/IEC 27001:2013(E)).

The Dictionary of Military and Associated Terms (2017) defined *human factors* as the psychological, cultural, behavioral, and other human attributes that influence decisionmaking, the flow of information, and the interpretation of information by individuals or groups.

The Merriam-Webster dictionary (2017) stated a *framework* is a basic conceptional structure (as of ideas), a skeletal, openwork or a structural frame.

The Fraud Diamond Theory was first presented by Wolfe and Hermanson (Wolfe and Hermanson, 2004), which is an expanded version of the Fraud Triangle Theory (FTT) of Cressey (1950), stated that to occur a fraud four elements are necessary: (i) perceived pressure, (ii) opportunity, and (iii) rationalization and (iv) capability. This theory is applicable to information security breaches as well.

METHODOLOGY

The primary data is collected from a survey of faculty members as library and information users with the help of online questionnaire created in Google forms. We used simple random sample of faculty members from colleges and universities across Mumbai region as library and information users. The secondary data is used to create the list of various aspects of human factor related to information security in university library. In order to realize the objectives and scope of this article, we checked the validity of these aspects of human factors using both primary and secondary data.

A framework provides a foundation or outline or a supporting structure which is useful for constructing the object around it. Some of the previous studies had provided frameworks of the human factors, which were used for different purposes. For this study we have considered five frameworks of human factors associated only with human safety and information security, which are:

1. Checklist items of Human Factors Area from European Organisation For The Safety Of Air Navigation (2004) [CIHFA]
2. Main human factors affecting information system security by Saeed Soltanmohammadi, Saman Asadi, Norafida Ithnin (2013) [MHFSS]
3. Human factors for an effective information security management system by Alavi, R., Islam, S., Jahankhani, H., & Al-Nemrat, A. (2013) [HFEIS]
4. Human aspects of information security framework by Parsons, Kathryn & McCormac, Agata& Butavicius, Marcus & Pattinson, Malcolm & Jerram, Cate. (2014).[HAISF]
5. The Human Factor Diamond framework developed by Areej Alhogail, Abdurrahman Mirza, Saad Haj Bakry (2015) [HFDF]

After detail study and analyzing all the human aspects mentioned in the framework are listed and relisted by omitting repetitive aspects and clubbing the common aspects together and to satisfy the first objective these human factors are divided as

1. human factor aspects- organizational
2. human factor aspects- individual

These listed aspects of human factor are validated by primary data collected from survey of sample population of faculty members across Mumbai region as users of library and information system. The percentage of faculty members who thought a particular aspect of human factor affects information security is mentioned.

For fulfilling the second objective we will try to trace the listed human aspects in the information security management standard 27001:2005 and 27001:2013. And further we will try to classify the listed human aspects by different categories to fulfil the third objective.

LITERATURE REVIEW

Waley and others (2012) in their research determined that human factors are responsible for 80-90% of information security breaches. Skorodumov and others (2015) considered social and human aspects in criminality growth and ultimately leading to complexity of methods and measures for information security. Majid and others (2015) stated that the human factor is the weakest link in information security and it is due to their lack of security awareness. Human factors cause

the greatest single issue of concern in ISMS (Jahankhani, et al. 2008).

Information security awareness as an aspect of human factor in information is studied by many researchers. The security awareness creation is considered as fifth step in the information System Security assessment Model (LISSAM) by Ismail and Zainab (2011). Waley and others (2012) identified awareness, motivation, communication, reinforcement, rewards and sanctions as five factors significantly affecting information security. Bauer, Benroider and Chudzikowski (2017) planned information awareness programs to find users compliance with the respective organization's information security policies.

Ethical environment, responsibility, people's values shaping information security management objectives were studied by Dhillon and Torkzadesh (2006). Karleson, Astrom and Arleson (2015) addressed information security culture for end users development. Rostogi and von Solms (2012) had discussed about importance of information security service culture in organizations for the end users. Govender, Kritzinger and Loock (2016) had studied the impact of national information security culture on strength of organization's information security. Sari and Nadiaolhaq (2016) found the information security also depends on people's understanding about the things required to be protected.

Gundu and Flowerday emphasized on behavioral intentions. Humaidi and Balakrishnan (2015) had studied influence of leadership styles on organizational information security. White, Hewitt and Kruck (2013) emphasized on information system security training in universities as national priority, considering today's graduates as tomorrow's information users and protectors.

Thus, many researchers conducted studies on a few aspects on human factors related to information security, all of those also applicable to university libraries. However for holistic information security management and policy making purpose the university librarian or the incident response team or the advisory board of professionals require to consider all those aspects related to human factors which affect information security of university library. Though many researchers had considered information security standards within their study, none of those actually checked the compliance of human factors with information security management standards.

Analysis of the frameworks of the human factors issues

Alhogail and others (Alhogail and others, 2015) had developed HFDF framework keeping in view the factors influencing employees' behavior with two domains each in "organization" dimension and "employee" dimension. Each dimension includes two domains and all these domains are interconnected forming a diamond shape.

Table 1 List of aspects of human factor

Sl. No.	Aspects of Human Factor	Frameworks				
		CIHFA	MHFSS	HFEIS	HAISF	HFDF
1	Apathy			√		
2	Attitude towards policy and procedures				√	√
3	Awareness			√	√	√
4	Budget			√		
5	Preparedness for change of old practices					√
6	Commitment					√
7	Controller communication, interaction, direction	√		√		√
8	Demographic				√	
9	Documentation and procedures for reporting, review and feedback	√				
10	Education of employee			√	√	√
11	Employee's individual culture/ character/ psychology			√	√	
12	Employee's irrational behavior in personal interest			√		
13	Employee's performance appraisal		√			√
14	Errors			√		
15	Experience	√		√	√	
16	Health hazard assessment	√				
17	Human-machine interaction- task and interface design	√				
18	Ignorance and negligence			√		
19	Individual learning, knowledge acquisition		√			√
20	Knowledge of policy and procedures understanding				√	
21	Management support and responsibilities		√	√		
22	Organization's security culture/ social norms/ workplace environment	√	√	√	√	√
23	Organizational security policy enforcement		√	√		√
24	Organizational Subjective norms – monitoring and control				√	√
25	Perceptions of employee					√
26	Organizational Practices and standards					√
27	Reward/ penalty	√	√	√	√	√
28	Roles and responsibilities acceptance	√		√		√
29	Rules and regulations					√
30	Skills/ proficiency/ competencies/ Self-efficacy			√	√	√
31	Staffing/ Manpower strength – personnel management	√				√
32	Stress			√		
33	System safety for human	√				
34	Teams factors and communication, interaction	√		√		√
35	Termination/ changes of employee's responsibilities					
36	Training and development	√	√		√	√
37	Workplace design	√				

MHFSS by Soltanmohammadi and others (Soltanmohammadi and others, 2013) had proposed the framework based on three factors - motivational, organizational and learning. They had derived these factors from Embrey's Classification of Human Errors, which described three categories of human error behavior are Skill-based errors, Rule-based errors and Knowledge-based errors (Embrey, 2005).

Alavi and others (Alavi and others, 2013) had formed HFEIS on the basis of SWOT analysis of two security incidents happened in UK financial organizations. The authors identified number of human factors related to human errors, awareness, communication, knowledge and character. All the identified human factors were divided into direct factors and indirect factors.

The European Organisation for the Safety of Air Navigation (European Organisation for the Safety of Air Navigation, 2004) formed the checklist items of six human factors areas based on stages of common structure of human factor case in various phases of system lifecycle reflecting the potential impacts on the performance of human as well as system.

Parsons and others (Parsons and others, 2014) developed the human aspects of information security model by reviewing number of information security policies, interviews of their senior management and an information security survey. They identified seven focus areas and three and three representative areas.

The various aspects of human factors accommodated in these above frameworks were analyzed and congregated together in table-1.

Aspects of human factor in compliance with Information Security Management Standards and users survey

The human factors listed in table-1 derived from various human factors frameworks are classified into two groups- organizational human factor aspects related to university libraries and human factor aspects related to individuals in table-2. Further these aspects are checked for their compliance with the information security management standards ISO/ISE 27001:2005 and ISO/ISE 27001:2013. To check the validity of the human factors, a survey was conducted of college faculties from across Mumbai region as information users. In total 159 responses were received for the survey. The percentage of faculty members who thought the particular aspect of human factor affects information security is mentioned in table-2. The table -2 makes it easy to compare aspects of human factor in compliance with Information Security Management (ISM) Standards and primary data collected from the survey.

Findings of the study

In total, 37 aspects of human factor were traced from frameworks of human factors associated only with human safety and information security. Out of 37 sorted human factors 17 were individual human factors and 20 were human factors within the organization's purview.

Table 2 Aspects of human factor in compliance with Information Security Management (ISM) Standards and users survey

Sl. No.	Aspects of Human Factor	Organizational (O) / Individual (I)	compliance with the ISM standards	Library and Information users agreed (% of users)
1	Apathy	I		79.1
2	Attitude towards policy and procedures	I	√	88.4
3	Awareness	O	√	72.1
4	Budget	O	√	81.4
5	Preparedness for change of old practices	I	√	93
6	Commitment	I	√	93
7	Controller communication, interaction, direction	O	√	88.4
8	Demographic	O		65.1
9	Documentation and procedures for reporting, review and feedback	O	√	88.4
10	Education of employee	I	√	86
11	Employee's individual culture/ character/ psychology	I	√	90.7
12	Employee's irrational behavior in personal interest	I		81.4
13	Employee's performance appraisal	O		81.4
14	Errors	O	√	74.4
15	Experience	I	√	86
16	Health hazard assessment	O		62.8
17	Human-machine interaction- task and interface design	O	√	79.1
18	Ignorance and negligence	I		69.8
19	Individual learning, knowledge acquisition	I	√	95.3
20	Knowledge of policy and procedures understanding	I	√	93
21	Management support and responsibilities	O	√	88.4
22	Organization's security culture/ social norms/ workplace environment	O	√	88.4
23	Organizational security policy enforcement	O	√	90.7
24	Organizational Subjective norms – monitoring and control	O	√	88.4
25	Perceptions of employee	I		86
26	Organizational Practices and standards	O	√	90.7
27	Reward/ penalty	O	√	86
28	Roles and responsibilities acceptance	I	√	93
29	Rules and regulations	O	√	90.7
30	Skills/ proficiency/ competencies/ Self-efficacy	I	√	93
31	Staffing/ Manpower strength – personnel management	I	√	79.1
32	Stress	I		74.4
33	System safety for human	O	√	83.7
34	Teams factors and communication, interaction	I		86
35	Termination/ changes of employee's responsibilities	O	√	76.7
36	Training and development	O	√	90.7
37	Workplace design	O	√	90.7

Termination or changes of employee's responsibilities, one of the important human factor mentioned in information security management standards, is not considered in any of the above mentioned five frameworks. The ISMS ISO 27001 of 2005 and 2013 did not consider psychological, demographic, behavioral, perceptional, stress, team work related issues of employees.

The most sought after human factors in the frameworks were organization's security culture, reward/ penalty, training and development. The more used or traced human factors in the frameworks were awareness, communication, education of employee, experience, organization's security policy enforcement, roles and responsibilities acceptance, skills and competencies and team aspects.

Checking of the factors compliance with the information security management standards ISO/ISE 27001:2005 and ISO/ISE 27001:2013 provides an idea about where the university library needs to emphasis when dealing with information security.

The survey indicated apathy, demographic and ignorance and negligence aspects of human factor, which were also not traced in standards, were least agreed upon by library and information users. Whereas, the users significantly agreed that employee's irrational behavior in personal interest, employee's performance appraisal and perceptions of employee are important aspects of human factor, but are not mentioned in the standards. According to users' survey Individual learning, knowledge acquisition, Preparedness for change of old practices, commitment, Knowledge of policy and procedures understanding, roles and responsibilities acceptance, Skills/ proficiency/ competencies/ Self-efficacy are the most important aspects of human factor for information security management in academic libraries.

Classification of Human aspects

From the literature review and human factors frameworks the following classification patterns are apparent. The classification patterns of human factors were based upon either cause and effect or organization and management.

1. Cognitive factors, behavioral factors, Environmental factors (From HFDF)
2. Organizational factors, individual (or personal) factors
3. Organizational factors, motivational factors and learning (From MHFSS)
4. Individual, Team, Management, Customer/clientele
5. Human assets factor (protector), Human threat Factor (intruder)
6. Direct factors, indirect factors (From HFEIS)
7. Individual, organizational, intervention (From HAISF)
8. Inherent characteristics, situational characteristics or factors

Significance of the study

All the problems of information security management begin with human factors and end with human factors. Hence the human factor is the main component of information security management besides technology. The significance of this study is as follows:

- As per literature review many studies of information security management had considered various human factors, but not considered all the aspects of human factors together, may be because of the wider scope. This paper tried to bring all human aspects associated with information security in university libraries together under one umbrella, giving a holistic approach to human factors, though not comprehensive.
- This paper will be useful for further research where human factors associated with information security management in university libraries are involved.
- It is also useful in any other research in management or library and information science, where consideration of human factors is necessary.

CONCLUSION

This paper has tried to provide a holistic overview of human factors in a nutshell in information security management for university libraries.In total we had traced 37 aspects of human factor and checked those aspects compliance with the information security management standards ISO/ISE 27001:2005 and ISO/ISE 27001:2013. The human aspects not mentioned in the standards are required to be taken care of at the organizational level. We have also checked the validity of these aspects of human factor in ISMS with the help of a survey of faculties as library and information users'. Both these results were put together for comparison purpose and more clarity. Thus, this paper is useful for researchers considering human factors in their research on information security management in university libraries. This paper is also useful for research in library and information science and human resource management, where human factors are considered.

References

Alavi, R., Islam, S., Jahankhani, H., & Al-Nemrat, A. (2013). Analyzing human factors for an effective information security management system. *International Journal of Secure Software Engineering (IJSSE)*, *4*(1), 50-74.

Alhogail, A., Mirza, A., & Bakry, S. H. (2015). A comprehensive human factor framework for Information Security in organizations. *Journal of Theoretical and Applied Information Technology*, *78*(2), 201.

Aware, Which They Are, To Provide Supporting Documentation, And Commercial Logical (2005). Information technology–Security techniques–Information security management systems–Requirements.

Bauer, S., Bernroider, E. W., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security*, *68*, 145-159.

Checklist items of Human Factors Area from European Organisation For The Safety Of Air Navigation (2004) retrieved on 21/9/17 from https://www.eurocontrol.int/sites/default/files/content/documents/nm/safety/safety-the-human-factors-case-guidance-for-human-factors-integration-2004.pdf

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in

organizations. *Information Systems Journal*, *16*(3), 293-314.

Dictionary of Military and Associated Terms retrieved on 23/1/17 from http://www.definitions.net/ definition/ human%20factors

E-Government Act of 2002. PUBLIC LAW 107-347—DEC. 17, 2002. *Federal Information Security Management Act of 2002*. [Online] [Cited: October 10, 2015.] http://www.gpo.gov/fdsys/pkg/STATUTE-116/pdf/STATUTE-116-Pg2899.pdf .

Embrey, D. (2005). Understanding human behaviour and error. Human Reliability Associates, 1, 1-10 in Soltanmohammadi, S., Asadi, S., & Ithnin, N. (2013). Main human factors affecting information system security. *Interdisciplinary Journal of Contemporary Research in Business*, *5*(7), 329-354.

Govender, S., Kritzinger, E., & Loock, M. (2016, May). The influence of national culture on information security culture. In *IST-Africa Week Conference, 2016* (pp. 1-9). IEEE

Gundu, T., & Flowerday, S. V. (2013). Ignorance to awareness: Towards an information security awareness process. *SAIEE Africa Research Journal*, *104*(2), 69-79.

Humaidi, N., & Balakrishnan, V. (2015). Leadership Styles and Information Security Compliance Behavior: The mediator effect of information security awareness. *International Journal of Information and Education Technology*, *5*(4), 311.

Ismail, R., & Zainab, A. N. (2013). Information systems security in special and public libraries: an assessment of status. *arXiv preprint arXiv:1301.5386*.

Karlsson, F., Åström, J., & Karlsson, M. (2015). Information security culture - state-of-the-art review between 2000 and 2013. *Information and Computer Security, 23*(3), 246-285.

Majid, H. A., Majid, M. A., Ibrahim, M. I., Manan, W. N. S. W., & Ramli, M. R. (2015, April). Investigation of security awareness on e-learning system among lecturers and students in Higher Education Institution. In *Computer, Communications, and Control Technology (I4CT), 2015 International Conference on* (pp. 216-220).IEEE

Merrium –Webster Dictionary retrieved on 23/1/17 from https://www.merriam-webster.com/ dictionary/framework

Ministry of human resource development, all India survey on higher education 2015-16. Retrieved on 2/10/17 from http://mhrd.gov.in/sites/upload_files/mhrd/ files/statistics/AISHE2015-16.pdf)

Parsons, Kathryn & McCormac, Agata & Butavicius, Marcus & Pattinson, Malcolm & Jerram, Cate. (2014). Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security.42. 10.1016/j.cose.2013. 12.003.

Rastogi, R., & von Solms, R. (2012). Information Security Service Culture-Information Security for End-users. *J. UCS*, *18*(12), 1628-1642.

Sari, P. K., & Nurshabrina, N. (2016, April). Factor analysis on information security management in higher education institutions. In *Cyber and IT Service Management, International Conference on* (pp. 1-5). IEEE.

Skorodumov, B. I., Skorodumova, O. B., & Matronina, L. F. (2015). Research of Human Factors in Information Security. *Modern Applied Science*, *9*(5), 287.

Soltanmohammadi, S., Asadi, S., & Ithnin, N. (2013). Main human factors affecting information system security. *Interdisciplinary Journal of Contemporary Research in Business*, *5*(7), 329-354.

The standardization committee INB/NK 149. SN ISO/IEC 27001:2013(E) - Information technology - Security techniques - Information security management systems - Requirements. Geneva, ISO copyright office, Nov 2013.

Waly, N., Tassabehji, R., & Kamala, M. (2012). Measures for improving information security management in organisations: the impact of training and awareness programmes. *UK Academy for Information Systems Conference Proceedings 2012. Paper 8* (pp. 1 - 10). Bradford: UK Academy for Information Systems UKAIS.

White, Garry L, Hewitt, B., & Kruck, S. E., (2013). Incorporating global information security and assurance in I.S. education. *Journal of Information Systems Education, 24*(1), 11-16.

Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal*, *74*(12), 38.

How to cite this article:

Shivarama J and Vaishali A. Dawar (2017) 'Aspects Human Factor For Information Security Management In Academic Libraries ', *International Journal of Current Advanced Research,* 06(11), pp. 7247-7252.
DOI: http://dx.doi.org/10.24327/ijcar.2017.7252.1109

****