Australian Journal of Basic and Applied Sciences
2019 October; 13(10): pages 99-107
DOI: 10.22587/ajbas.2019.13.10.14
Original paper
Journal home page: www.ajbasweb.com
AENSI Publications

Factors Effecting Information Security Management and their impacts on Organization performance in the work environment: Case study; Hatif Libya Company (HLC)

Jamal Elattresh[1], Khalid Ramadan[2], Umit Tokeser[3]

1Department of Computer Science, Institute of Materials and Engineering, Kastamonu University/Turkey
2Department of Computer Science, Institute of Materials and Engineering, Kastamonu University/Turkey
3Department of Mathematics, Faculty of Science and letters, Kastamonu University/Turkey

Correspondence Author: Jamal Elattresh, Department of Computer Science, Institute of Materials and Engineering, Kastamonu University/Turkey
E-mail:- *alatrashly@gmail.com*

Received date: 25 July 2019, Accepted date: 28 September 2019, Online date: 25 October 2019

Abstract

Information security (InfoSec) is an important issue which is gaining more and more interest by organizations worldwide. This study aims to evaluate the service management approach of information security management that applied and utilized to improve effective information security management in the Hatif Libya Company (HLC). The aim of this study is to evaluate the processes and the performance of HLC by following the improvements of information security management standards at the company.
This research study has used a descriptive research approach to collect the required data by designing and distributing an online questionnaire to the study participants. An interpretive case-study approach, as well as questionnaires, were employed to support data gathering. On the other hand, the researchers have reviewed previous studies that talked about subjects to compare among identifying the similarities as well as differences among related to the research topic. The discussion and analysis processes has been applied for the findings and results to evaluate the importance of considering information security management for HLC and Libyan related companies; and also, for those who are interested in the same study subject.
In conclusion, The main objective of this research, concepts and principles of information security have been tested to deliver actionable information for decision-makers within HLC firm to manage their corporate assets and ensure their resilience and increase productivity. In addition, this practical research study is an important for Libyan organizations as organizations are working at one of the development countries who they are seeking to ensure high level of information security management factors to increase company's performance and productivity to make time to market.

Keywords: Information security, Information security management system (ISMS), employee satisfaction, Protection and safety, performance and ability, risk management

INTRODUCTION

Information security framework (InfoSec) is a multi-layered structure, which empowers the change of info into outputs utilizing strategies and models (Mai et al., 2017); (Pal and Anand, 2018), while PC framework can be characterized as a feature of a data framework which has been automated. The data framework can be contrasted with the nervous system. Breaking down in one place can cause disappointment of the whole association and its presentation to the danger (Aiello, 2015); (Shameli et al., 2016). In this manner, keeping up a superior data framework, including the proper level of security may directly affect how associations react to crises according to some risk documentation and reports (Wawak, 2010); (Pal and Anand, 2018). Data security is characterized as shielding data and data frameworks from unapproved work environment get to, utilize, exposure, disturbance, alteration and pulverization (Andress, 2011; O'Brien and Marakas, 2005). In formation, security is uprightness, utility, and ownership as the basic attributes of data (O'Brien and Marakas, 2005). Data Security is an expert framework in anchoring data transmitted through the Internet from the dangers that debilitate it (Boehmer, 2008). Data security (InfoSec) is procedures and apparatuses planned and conveyed to shield business data from adjustment, interruption, obliteration and examination. Compelling data Security fuses security items, advancements, approaches (Pattinson et al., 2015), and also methods (Alberts and Dorofee, 2002; Boehmer, 2008).

Citation: Elattresh *et al.*, **Factors Effecting Information Security Management and their impacts on Organization performance in the work environment: Case study; Hatif Libya Company (HLC)**. Australian Journal of Basic and Applied Sciences, 13(10): 99-107. DOI: 10.22587/ajbas.2019.13.10.14

This paper organized as section one presented an introduction and research questions, section two literature review, section three the research methodology, section four the result and discussion; section five the conclusion.

1.1. Why HLC needs information security management?

The company was established by a decree of the Secretary of the Management Committee of the Libyan Post, Communications and data Techy Company (Holding the reference number (4)/2008. The purpose was to operate and maintain the sovereign frameworks, and to develop the national telephone network and data security management framework. It includes the local frameworks of transit dividers and subdivisions and interconnection means within cities. The company aims to contribute to building the economy of the society through the work it provides and to preserve the values, principles, and ideals of society. The company also inspires to create an environment to connect to the latest services and technologies. Hatif Libya company web page as presented in figure.1.1. below.

Figure. 1.1. Hatif Libya Company web page (source: https://hlc.ly).

1.2. Research Questions

The overall goal of the present study is to analyze factors that influence on information security management at H LC. The following are research questions that guided the study;

1. To what extent there is an argument between end-utilizers and information security managers on the effectiveness of information security in the organization?

Sub Questions:

1.1. Is there a statistically significant difference between the end-utilizers and information security managers in the information security policies and controls?

1.2. Is there a statistically significant difference between the end-utilizers and information security managers in the Protection and safety skills?

1.3. Is there a statistically significant difference between end-utilizers and information security managers in client satisfaction?

1.4. Is there a statistically significant difference between the end-utilizers and information security managers background about the information security concerns?

1.5. Is there a statistically significant difference between the end-utilizers and information security managers in supportability and accessibility?

1.6. Is there a statistically significant difference between the end-utilizers and information security managers in awareness of risks and documentations?

1.3. Research Objectives

1. To Understand the information security behaviors of end-users in Hatif Libya Company.
2. To identify the awareness degree of end-utilizers for their own role in the protection of information and how to behave in order to fulfill this role in the organization.
3. To identify the compliance of end-utilizers with the information security policies and controls in the Hatif Libya Company.
4. To identify a management approach that has the potential to resolve any problem caused by the end-users in the organization.

2. LITERATURE REVIEW:

As indicated by Al-Mabrouk and Soar (2009), exchange of data innovation is an undeniably imperative segment for techno-monetary improvement in creating nations. However, according to Disterer (2013), there have been almost no investigations in IT move in producing nations, for example, Arab nations. The achievement of the IT exchange process relies on various issues that must be recognized for every nation. Twati and Gammack (2006) declared that data is a standout amongst the most imperative components of business administration at the Libyan organization. Disterer (2013) states that with the expanding of the criticalness of data innovation, and there is an earnest requirement for satisfactory proportions of data security management. Murugiah and Akgam (2015); Alhgig and Mehta (2018); Bezweek and Egbu (2009) has pronounced that a helpful commitment of information security practices as there are just a couple of studies managing the appraisal of data security and administration quality in the saving money of Libya. The discoveries depended on three diverse free factors benefit quality, client dedication and security which demonstrated that every one of these factors impacted buyers fulfilment in the Libyan managing an account

Citation: Elattresh *et al.*, **Factors Effecting Information Security Management and their impacts on Organization performance in the work environment: Case study; Hatif Libya Company (HLC)**. Australian Journal of Basic and Applied Sciences, 13(10): 99-107. DOI: 10.22587/ajbas.2019.13.10.14

segment as well as information security management frameworks. Libyan E-government should enhance all sites of the legislature and instruct government workers to increase productivity and employee performance.

In 2013, protestors stormed the headquarters of the Libya Telecom and Techy and information security management requesting and compelling engineers to cut off web access across large parts of the nation to obstruct accessing the online administrations, as online dangers and vicious assaults on journalists increased. Benghazi was cut off from all telecom frameworks for a while in 2015. Saw Gross domestic product (GDP) fall drastically as of late and looks set to proceed into (2017), has obstructed the capacity of Telco's to put resources into the foundation. Web infiltration has customarily been low in Libya. As per figures from the International Telecommunication Union, web infiltration enhanced via one rate point from 2015 to 2016, from 20 to 25% of Libyans. This ascent might be associated with better 3G inclusion, increment data security administration, and lower costs. Kenan et al. (2011) stated that there is a connection among hierarchical culture developments and the reception of data security administration in Libya.

Moreover, Libya needs to build up a nearby relationship with mechanically and advanced nations, for example, the US and the UK, to make the coveted progress and high level of information management system usage (Busoud and Zivkovic, 2016). In 2012, the Libyan government made concurrences with the UK to help in the improvement of the essential social communication and internet transmission and telecommunication and ensuring privacy and security issue establishments (Maumbe et al., 2008); (Aladwani, 2003). Hatif Libya company (HLC) needs to be adapted this techy and execute it over the entire organization with the end goal to enhance the correspondence among the legislature and the residents or individuals to individuals, people to an association inside or outside Libya. The utilization of data security administration permits Hatif Libya organization to find what the workers or clients need and how to fulfill their necessities; besides, it ensures media transmission and protection amid users of Hatif Libya (Radwan, 2013). Amanullah et al. (2005) have investigated that control framework deregulation expedites more extensive dependence data frameworks and media transmission framework to share the basic and non-basic information. Manochehri et al.(2012) stated that data and correspondence innovations, and also data security are broadly utilized via organizations to improve firms aggressiveness.

3. METHODOLOGY

This study utilized a descriptive research methodology which is suitable for this sort of research study (Kumar, 2019). The study will utilize a mixed-method research design utilizing quantitative and qualitative approaches (Colorafi and Evans, 2016). Therefore, research methods, questionnaires and interviews, were used to collect the required data which can adequately address the research questions. Research participants completed an online questionnaire (Survey Monkey source https://www.surveymonkey.com/). The questionnaire data were analyzed quantitatively utilizing SPSS software (Subramani and Kumar, 2018).

3.2 The Target sample

The participants of this research were the employees of the HLC. Participants were Libyan Hatif Libya firm employees and managers, who worked and were responsible for information security management of Hatif Libya firm. The total number of participants was 201. As presented in Figure.1.2.below the model of analysis. This study had taken as a sample of the gathered data to perform the reliability test which is a suitable way to this kind of data analysis.

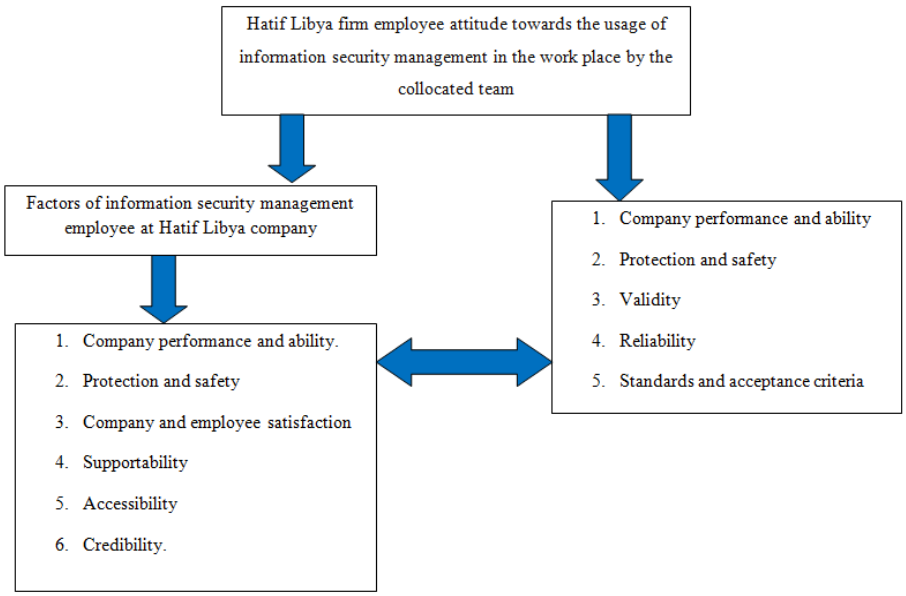

Figure.1.2. The model of analysis.

4. RESULT

4.1 Statistical Analysis

Citation: Elattresh *et al.*, **Factors Effecting Information Security Management and their impacts on Organization performance in the work environment: Case study; Hatif Libya Company (HLC)**. Australian Journal of Basic and Applied Sciences, 13(10): 99-107. DOI: 10.22587/ajbas.2019.13.10.14

The statistical analyses performed were; correlational analysis, which was utilized by means of SPSS software program.

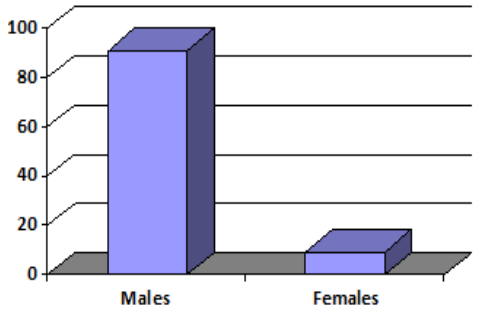

Figure.1.3.The participant distribution according to Gender

.

4.2 Descriptive statistics of study variables

Table.1.1. The descriptive statistics of Security Policies and Control and its items

Descriptive Statistics			
	N	Mean	Std. Deviation
F1: Security Policies and Control	133	3.75	.74015
17 Use encryption mechanisms to protect data and information:	137	3.80	1.058
22 Information security policy and method are periodically reviewed and improved:	137	**3.56**	1.090
23 Training staff on information systems periodically to develop their skills and raise the level of performance in security developments:	137	**3.56**	1.254
25 The employment terms of the company are to sign a contract not to disclose any sensitive information concerning the company:	137	3.85	.999
26 Employees are required to report any weaknesses they may see in the company's information systems:	137	**3.99**	.951
27 There is a regulatory record to track user activities and information security incidents within the company:	137	3.82	.941
30 An agency responsible for the management of the company supervises information security policies within the company:	137	3.75	.945
42 There are plans to restore the business to normal following a specific time frame and in case of any failures or interruptions in the information security management within the company and its subsidiaries:	133	3.65	.993
Valid N (listwise)	133		

Table.1.2. The descriptive statistics of Protection and safety skills and items.

Descriptive Statistics			
	N	Mean	Std. Deviation
F2: Protection and safety skills	133	3.72	.86733
29 The Company has written policies and procedures to manage the security of the information and its operating systems:	137	3.63	1.098
31 The senior management of the company is fully aware of the importance of the information systems security management policy with the presence of preventive measures in the implementation of any changes to information systems to protect them from risk:	137	**3.90**	.877
40 There is a directory for the classification of information that can help the employee to renew how information is handled and protected	133	**3.62**	1.140
Valid N (listwise)	133		

Table.1.2. Presents the descriptive statistics of the factor 2 which presented in F2: Protection and safety skills and its items. The highest thing is item 31. This shows that the senior management of the company is fully aware of the importance of the information systems security management policy with the presence of preventive measures in the implementation of any changes to information systems to protect them from risk (M = 3.90, SD = .877). The lowest item is 40, which indicates that there is rarely

Citation: Elattresh *et al.*, **Factors Effecting Information Security Management and their impacts on Organization performance in the work environment: Case study; Hatif Libya Company (HLC)**. Australian Journal of Basic and Applied Sciences, 13(10): 99-107. DOI: 10.22587/ajbas.2019.13.10.14

a directory for the classification of information that can help the employee to renew how data is handled and protected (M = 3.62, SD = 1.140).

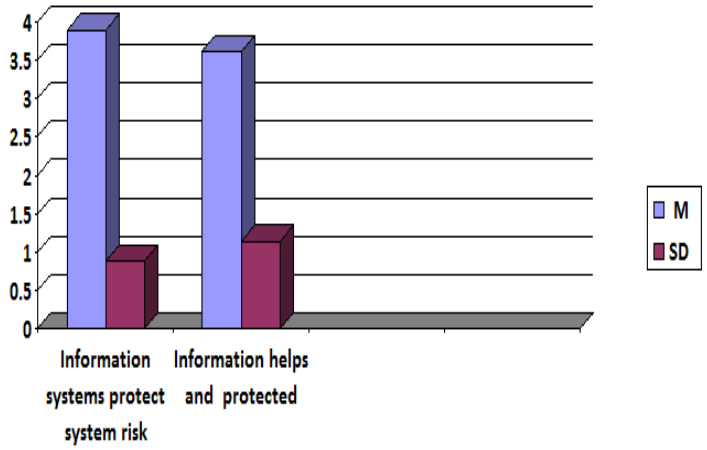

Figure.1.4. The descriptive statistics of Protection and safety skills and items.

Table.1.3. The descriptive statistics of Client satisfaction factor.

Descriptive Statistics			
	N	Mean	Std. Deviation
F3: Client satisfaction	137	2.52	.74722
7 The extent of the company's use of electronic information systems in performing its functions and providing its services:	137	**2.80**	.956
8 The presence of a competent department to manage the security of the company's information systems:	137	2.62	1.023
9 The level of training in the field of information security management compared to the systems operating in the company:	137	**2.20**	.971
10 The percentage allocated to spend on management procedures and the protection of information and operating systems compared to the general expenses of the company:	137	2.47	1.000
Valid N (listwise)	137		

Table.1.4. The descriptive statistics of the knowledge about IS Concerns.

Descriptive Statistics			
	N	Mean	Std. Deviation
F4: The knowledge about IS Concerns	133	4.00	.68595
32 The powers of access to information systems are given according to the administrative and functional position assigned to the concerned employee:	135	**4.15**	.851
33 There are no general accounts and powers used by several employees, each employee has his specific account accessibility:	135	**3.91**	.934
41 The events that lead to the discontinuation of the information systems in the company are identified and documented, and the assessment and risks resulting from those events are to establish contingency plans to ensure the restoration of work:	133	3.95	.928
Valid N (listwise)	133		

Table.1.4. shows descriptive statistics of F4 the knowledge about IS Concerns and its items. The highest item is item 32. This affirms that the powers of access to information systems are given according to the administrative and functional position assigned to the concerned employee (M = 4.15, SD = .851). The lowest item is item 33, which shows that there are no general accounts and powers used by several employees, each employee has his specific account accessibility (M = 3.91, SD = .934).

Citation: Elattresh *et al.*, **Factors Effecting Information Security Management and their impacts on Organization performance in the work environment: Case study; Hatif Libya Company (HLC)**. Australian Journal of Basic and Applied Sciences, 13(10): 99-107. DOI: 10.22587/ajbas.2019.13.10.14

Table.1.5. The descriptive statistics of Supportability and Accessibility

Descriptive Statistics			
	N	Mean	Std. Deviation
F5: Supportability and Accessibility	135	3.74	.74532
35 Most sensitive information systems within the company's departments and branches are isolated via a local private network (LAN):	135	**3.96**	.999
36 Access to the Internet sometimes obscures the Internet through the company's information systems:	135	3.69	1.054
37 There are guidelines for how to create strong passwords for information systems:	135	3.61	1.139
38 In the company information systems operating the user's powers are closed after a specified period of lack of activity:	135	**3.53**	1.125
39 Performance records are used to store user activities and information for reasons of security and confidentiality of information	135	3.90	.900
Valid N (listwise)	135		

Table.1.5.above has presented descriptive statistics of F5: Supportability and Accessibility and its items. The highest item is item 35, where sensitive information systems within the company's departments and branches are isolated via a local private network (LAN) (M = 3.96, SD = .999). The lowest item is item 38: this particular result appoints that in the company information systems operating the user's powers are closed after a specified period of lack of activity (M = 3.53, SD = 1.125).

Table.1.6. The descriptive statistics of Awareness of Risks and documentations

Descriptive Statistics			
	N	Mean	Std. Deviation
F6: Awareness of Risks and documentations	137	3.92	.75612
11 The use of security requirements, for instance, walls - doors - locks – cards to protect the components of the company's:	137	3.94	.961
12 Power and communication cables that transmit data or support servers Information systems are protected against tampering or destruction:	137	3.86	1.001
13 The presence of an alternative electric power source in the company:	137	4.03	.977
14 Maintain the equipment of the company properly to ensure its continuity and safety:	137	3.89	1.089
15 Any employee who is not qualified eliminated from making any material or moral changes to the devices operating within the company's information systems	137	**4.08**	.993
18 Provide the backup service	137	3.90	1.087
19 The databases used in the company system provide multiple security levels:	137	3.87	1.006
20 Using protection programs to track penetration and infiltration:	137	**3.76**	1.081
Valid N (listwise)	137		

Table 1.6. Has presented descriptive statistics of F6: Awareness of Risks and documentations and its items. In additions, the table depicts that the highest item is item 15, as any employee who is not qualified eliminated from making any material or moral changes to the devices operating within the company's information systems (M = 4.08, SD = .993). The lowest item is item 20: Using protection programs to track penetration and infiltration (M = 3.76, SD = 1.081).

4.3 Correlations between variables

Pearson Correlation was calculated between factors of information security management (Security Policies and Control, Protection, and safety skills, Client Satisfaction, The knowledge about IS Concerns, Supportability and Accessibility, Awareness of Risks and documentations) and information security management providers' perceptions and attitudes towards the use of information security management at workplace. Results are presented below. As shown in Table 4.15 below, positive significant correlations were found between security policies and control and Client Satisfaction and Awareness of Risks and documentations (.366 and .698 respectively), $p < .01$. Protection and safety skills correlate significantly and positively with Client Satisfaction, The knowledge about IS Concerns, Supportability and Accessibility and Awareness of Risks and documentations (.391, .420, .545 and .334 respectively), $p < .01$. Client Satisfaction, in additions, correlated in the same manner (.253, .316 and .318 respectively). Moreover, the knowledge about IS Concerns and Supportability and Accessibility had significant and strong positive correlations with Awareness of Risks and documentations (.698 and .538 respectively), $p < .01$. In additions, the support can be added to the suggested model and encourage tests of predictors of Client Satisfaction analysis. In Table 4.15, the Correlations test and factors Pearson Correlation was calculated between factors of information security management (Security Policies and Control, Protection and safety skills, Client Satisfaction, The knowledge about IS Concerns, Supportability and Accessibility, Awareness of Risks and documentations) and information security management providers' perceptions and attitudes towards the use of information security management at workplace. Results are presented as below.

Citation: Elattresh *et al.*, **Factors Effecting Information Security Management and their impacts on Organization performance in the work environment: Case study; Hatif Libya Company (HLC)**. Australian Journal of Basic and Applied Sciences, 13(10): 99-107. DOI: 10.22587/ajbas.2019.13.10.14

As shown in Table 4.15 positive significant correlations were found between Security Policies and Control and Client Satisfaction and Awareness of Risks and documentations (.366 and .698 respectively), p < .01. Protection and safety skills correlate significantly and positively with Client Satisfaction, The knowledge about IS Concerns, Supportability and Accessibility and Awareness of Risks and documentations (.391, .420, .545 and .334 respectively), p < .01. Client Satisfaction, in additions, correlated in the same manner (.253, .316 and .318 respectively). The knowledge about IS Concerns and Supportability and Accessibility had significant and strong positive correlations with Awareness of Risks and documentations (.698 and .538 respectively), p < .01. In additions, the support can be added to the suggested model and encourage tests of predictors of Client Satisfaction analysis.

Table.4.15. The Correlations test and factors

Correlations							
		F1	F2	F3	F4	F5	F6
F1- Security Policies and Control	Pearson Correlation	1					
	Sig. (2-tailed)						
	N	133					
F2- Protection and safety skills	Pearson Correlation	.647**	1				
	Sig. (2-tailed)	.000					
	N	133	133				
F3- Client Satisfaction	Pearson Correlation	.366**	.391**	1			
	Sig. (2-tailed)	.000	.000				
	N	133	133	137			
F4- The knowledge about IS Concerns	Pearson Correlation	.535**	.420**	.253**	1		
	Sig. (2-tailed)	.000	.000	.003			
	N	133	133	133	133		
F5- Supportability and Accessibility	Pearson Correlation	.631**	.545**	.316**	.527**	1	
	Sig. (2-tailed)	.000	.000	.000	.000		
	N	133	133	135	133	135	
F6- Awareness of Risks and documentations	Pearson Correlation	.698**	.334**	.318**	.457**	.538**	1
	Sig. (2-tailed)	.000	.000	.000	.000	.000	
	N	133	133	137	133	135	137
**. Correlation is significant at the 0.01 level (2-tailed).							

5. DISCUSSION

The main objective of this study is to identify the effects of the research factors on information security management at Hatif Libya Company (HLC). Most of the respondents were males and their age ranging between 40 and 49 years, and the majority has Bachelor education degree and based on this critical point they need to be trained and improve their education level based on the research information that collected from the target sample. Moreover, Table.4.4 presented the distribution of participants according to years of experience; 23.4% of participants have less than 5 years of experience, 21.9% have from 5 to less than 10 years, 17.5% have from 10 to less than 15 years and 37.2% have 15 years and above which is reflects that the majority of the HLC employees are experienced about the company difficulties and they can solve the majority of the information security problems that can face the company during the company work environment performance (Pal and Anand, 2018) based on the security of the telecommunication and the first factor of this research study and similar to (Soomro et al, 2016) Data Experts/Managers in functional areas have day-t-day responsibilities for managing company transactions processes (Aiello, 2015), establishing business rules for the production transaction system as related to information security as well as maintenance. After analyzing the data and testing the hypotheses, the study revealed that table.1.1 has represented the descriptive statistics of F1: Security Policies and Control and its items which is the most important factor (Pal and Anand, 2018) that should be considered at any telecommunication company such as HLC. The highest item is item 26; Employees are required to report any weaknesses they may see in the company's information systems management (M = 3.99, SD = .951) which is reflects that information security management policies and control should be taken in consideration (Shameli et al., 2016). The lowest items are 22; Information security policy and method are periodically reviewed and improved (M = 3.56, SD = 1.090) and 23; Training staff on information systems periodically to develop their skills and raise the level of performance in security developments (M = 3.56, SD = 1.254) which is similar to (Narain Singh et al 2014). Table.1.3. above shows descriptive statistics of F3: Client satisfaction and its items; in fact HLC firm should be considered such factor to ensure success in the workplace by applying modern information security standards (Hsu et al., 2016); (Huang et al., 2016). The highest item is item 7; the extent of the company's use of electronic information systems in performing its functions and providing its services (M = 2.80, SD = .956). The lowest item is item 9; the level of training in the field of information security management compared to the systems operating in the company (M = 2.20, SD = .971) as discussed by (Peltier, 2016). The most important factors are security policies and control and client satisfaction and awareness of risks and documentations which are similar to (Pattinson et al., 2015); (Shameli et al., 2016), protection and safety skills related to employee performance and education as reported at this study to improve employee education by taken some related courses and training in the terms of information security management.

6. CONCLUSION

This research study aimed to identify factors may interrupt information security management at HLC. Even though this research makes efforts to adopt multiple research approaches to strengthen the validity of the research findings, comparatively larger sample size in a survey would have been more beneficial. Getting information security-related data from the employees of Hatif Libya company remains a big point of challenging. Time, as well as company resources based on information security requirements (Pal and Anand, 2018), are the obvious constraints in getting such research information.

Moreover, the responses to identified information security management factors are contextual and consequently, further research effort is required to test the findings in different settings. Second, the present study only aims to identify some information security management factors according to HLC as a firm that considered as one of the developing countries. After data analysis and hypotheses testing, the results show that all the research factors have a significant statistical influence on information security management at HLC; and there are some factors , for instance, employee education and performance, security policies and control, awareness of risks and documentations are an important to this firm as reported by this research study. In addition, the findings reaffirm that all the hypothesis factors have a positive significant correlations were found between security policies and control and client satisfaction and awareness of risks and documentations, protection and safety skills related to employee performance and education which are reflects the performance of a positive service that provided by HLC company while taken all the research factors in consideration that should be applied in HLC firm. Protection and safety skills correlate significantly and positively with client Satisfaction, The knowledge about IS Concerns, Supportability and accessibility and awareness of risks and documentations which need some training courses for the target sample to increase HLC performance and productivity. Client Satisfaction, in additions, correlated in the same manner. Finally, this study may suggest conducting further research to study more variables which may affect information security management such as trust, and usability.

REFERENCES

Al-Mabrouk, K., & Soar, J. (2009). A Delphi examination of emerging issues for successful information technology transfer in North Africa a case of Libya. African Journal of Business Management, 3(3), 107-114. ISSN 1993-823

Alhgig, N., & Mehta, R. (2018). A Study on Communications and Information Technology in Libya over the Past Decades. IOSR Journal of Business and Management (IOSR-JBM), e-ISSN: 2278-487X, p-ISSN: 2319-7668. Volume 20, Issue 3. Ver. VI (March. 2018), PP 07-11 , DOI: 10.9790/487X-2003060711, www.iosrjournals.org.

Aiello, M. (2015). End User Information Security: How InfoSec Literacy Affects Business. Aiello, M. (2015). End User Information Security: How InfoSec Literacy Affects Business. https://scholarsarchive.jwu.edu/mba_student/43

Amanullah, M. T. O., Kalam, A., & Zayegh, A. (2005). Network security vulnerabilities in SCADA and EMS. In Transmission and Distribution Conference and Exhibition: Asia and Pacific, 2005 IEEE/PES (pp. 1-6). DOI: 10.1109/TDC.2005.1546981, IEEE.

Aladwani, A. M. (2003). Key Internet characteristics and e-commerce issues in Arab countries. Information Technology & People, 16(1), 9-20. https://doi.org/10.1108/09593840310462998

Alberts, C. J., & Dorofee, A. (2002). Managing information security risks: the OCTAVE approach. Addison-Wesley Longman Publishing Co., Inc. ISBN:0321118863

Boehmer, W. (2008, August). Appraisal of the effectiveness and efficiency of an information security management system based on ISO 27001. In Emerging Security Information, Systems and Technologies, 2008. SECURWARE'08. Second International Conference on (pp. 224-231). DOI: 10.1109/SECURWARE.2008.7. IEEE.

Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2008). Information security and risk management. Communications of the ACM, 51(4), 64-68, ACM, 2008.

Bezweek, S. A., & Egbu, C. O. (2009). The impact of information technology in facilitating communication and collaboration in Libyan public organisations-a literature review. Managing IT in Construction/Managing Construction for Tomorrow, 461.

Busoud, A., & Živković, D. (2016). E-government in Libya. In International scientific conference on ict and e-business related research, https://doi.org/10.1007/s10209-017-0575-3.

Colorafi, K. J., & Evans, B. (2016). Qualitative descriptive methods in health science research. HERD: Health Environments Research & Design Journal, 9(4), 16-25. https://doi.org/10.1177/1937586715614171.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. Journal of Information Security, 4(02), 92. http://dx.doi.org/10.4236/jis.2013.42011.

Haimes, Y. Y. (2015). Risk modeling, assessment, and management. John Wiley & Sons.

Hsu, C., Wang, T., & Lu, A. (2016, January). The Impact of ISO 27001 certification on firm performance. In 2016 49th Hawaii International Conference on System Sciences (HICSS)(pp. 4842-4848). DOI: 10.1109/HICSS.2016.600 . IEEE.

Huang, K. E., Wu, J. H., Lu, S. Y., & Lin, Y. C. (2016). Innovation and technology creation effects on organizational performance. Journal of Business Research, 69(6), 2187-2192. https://doi.org/10.1016/j.jbusres.2015.12.028.

Kumar, R. (2019). Research methodology: A step-by-step guide for beginners. Sage Publications Limited.

Maumbe, B. M., Owei, V., & Alexander, H. (2008). Questioning the pace and pathway of e-government development in Africa: A case study of South Africa's Cape Gateway project. Government Information Quarterly, 25(4), 757-777. https://doi.org/10.1016/j.giq.2007.08.007.

Manochehri, N. N., Al-Esmail, R. A., & Ashrafi, R. (2012). Examining the impact of information and communication technologies (ICT) on enterprise practices: A preliminary perspective from Qatar. The Electronic Journal of Information Systems in Developing Countries, 51(1), 1-16. https://doi.org/10.1002/j.1681-4835.2012.tb00360.x.

Murugiah, L., & Akgam, H. A. (2015). Study of customer satisfaction in the banking sector in Libya. Journal of Economics, Business and Management, 3(7), 674-677. DOI: 10.7763/JOEBM.2015.V3.264.

Mai, B., Parsons, T., Prybutok, V., & Namuduri, K. (2017). Neuroscience foundations for human decision making in information security: a general framework and experiment design. In *Information Systems and Neuroscience* (pp. 91-98). Springer, Cham.

Narain Singh, A., Gupta, M. P., & Ojha, A. (2014). Identifying factors of "organizational information security management". Journal of Enterprise Information Management, 27(5), 644-667. ISSN: 1741-0398.

O'Brien, J. A., & Marakas, G. M. (2005). Introduction to information systems (Vol. 13). New York City, USA: McGraw-Hill/Irwin. ISBN-13: 978-0073376882.

Peltier, T. R. (2010). Information security risk analysis. Auerbach publications.

Pandey, M. K., Kumar, S., & Karthikeyan, S . (2016). Information Security Management System (ISMS) Standards in Cloud Computing-A Critical Review. ISSN 1857-7288.

Peltier, T. R. (2016). Information Security Policies, Procedures, and Standards: guidelines for effective information security management. Auerbach Publications. Boca Raton, FL 33487-2742.

Pal, S. K., & Anand, S. (2018). InfoSec: A Comprehensive Study. IUP Journal of Computer Sciences, 12(3).

Pattinson, M. R., Butavicius, M. A., Parsons, K., McCormac, A., & Jerram, C. (2015). Examining Attitudes toward Information Security Behaviour using Mixed Methods. In HAISA (pp. 57-70).

Prokupets, R., & Regelski, M. (2008). U.S. Patent No. 7,380,279. Washington, DC: U.S. Patent and Trademark Office. US7752652B2.

Radwan, R. (2013). E-Government: Libyan Plan towards Better Services. ISSN : 2248-9622.

Rowlingson, R., & Winsborrow, R. (2006). A comparison of the Payment Card Industry data security standard with ISO17799. Computer Fraud & Security, 2006(3), 16-19. https://doi.org/10.1016/S1361-3723(06)70323-2.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), 215-225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009.

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security*, *57*, 14-30. https://doi.org/10.1016/j.cose.2015.11.001.

Subramani, T., & Kumar, T. S. (2018). Analyzing Inventory Material Management Control Techniques on Residential Construction Project Using SPSS. *International Journal of Engineering & Technology*, *7*(3.10), 36-39.

Twati, J. M., & Gammack, J. G. (2006). The impact of organisational culture innovation on the adoption of IS/IT: the case of Libya. Journal of enterprise information management, 19(2), 175-191. https://doi.org/10.1108/17410390610645076.

Wawak, S. (2010). The Importance of Information Security Management in Crisis Prevention in the Company. https://mpra.ub.