An Investigation of the Information Security Awareness and Practices among Third Level Education Staff, Case Study in Nalut Libya

Hamida Asker, MSc
Nalut University, Libya
Abdalmonem Tamtam, PhD
Nalut University, Libya, Dublin City University, Ireland

Doi:10.19044/esj.2020.v16n15p20 URL:http://dx.doi.org/10.19044/esj.2020.v16n15p20

Abstract

The development of Information and Communication Technologies (ICTs) is becoming very common throughout society. Therefore, it is a must to protect information assets. In addition to the technological aspect, research continues to confirm the need to enhance security awareness among employees. The objective of this study is to investigate the factors that may impact users' practice and awareness both in the workplace. Specifically, factors such as policy, behavior, training, knowledge of IT and education were tested. In addition, the second objective of this study is to investigate the information security awareness and practice level among the employees. To achieve the study objectives, a quantitative methodology was applied; specifically a survey instrument was developed to measure if each of the key factors has a significant association within the security awareness and practice in the workplace. 202 usable surveys were collected from higher education employees and analyzed using Bivariate/Pearson Correlation to determine the relationship between the independent variable and the dependent variable. The findings of the study revealed that there was a positive correlation between policy, behavior, training, knowledge of IT and education with security awareness and practice These results indicated that security awareness and practice level of employees' in the workplace at the middle level. It is hoped that the present study provides an initial step to focus on security training sessions among higher education employees to reflect new knowledge on the importance of security training to increase the knowledge of information security.

Keywords: Security awareness, Security practice, Workplace user

1. Introduction

With the advancement of technology, higher education institutes face challenges to secure their information assets that could be vulnerable to breach of security. Information security issues are considered the top priorities in various organisations including those in academic sector. Computer security and crime are considered serious and challenging issues to the information system, protecting the assets of the information depends on the success of the information security plan and the execution of various security controls within the organisation (Alshamrani and Mehdim, 2012; Ahlan and Lubis, 2011).

In general, there is a considerable reliance on the human element in the field of information security in terms of behaviour and knowledge; this means that people who are engaged in work associated with information security must possess the necessary knowledge about protecting information and ensuring a high level of security of information (Kruger et al., 2011).

Information security issues were investigated as a technical problem for many years, without paying attention to the human factor and how security culture and awareness of information security affect users' behaviour in providing additional protection for information assets (Alfawaz et al., 2010).

Information security awareness minimizes the level of risks to information assets, specifically by reducing the risk of employee unwise behaviour and harmful interaction with information assets. With the rise of mobility and the effect of globalization, modern organisations require guidance in establishing information security aware or implementing an appropriately stringent information security culture (O'Brien et al., 2013). Therefore, the risk can be caused by the employees themselves regarding the security of information assets because of weak practicing and unawareness of information threats (Da Veiga & Eloff, 2010).

Employees in organisations who are also home users of computing technology are susceptible to security breaches unless they comply with the organisation policy to use safeguards such as firewalls and antivirus programs. Colleges and universities may be easily exposed to attacks by hackers for two reasons: the first reason is the open access provided by the university for students and guests while the second reason is the role of the staff and employees in protecting information systems within their organisations as classified information still possesses real concern for organisations (Ishak et al., 2014; Rezgui & Marks, 2008; Hazari et al., 2008).

In this study, the problem is to identify the effect of policy, behaviour, training, knowledge of IT, and education on employees' security awareness and practice in the workplace.

1.1 Study Questions:

1. How the factors of policy, behavior, training, knowledge of technology and education might influence the security awareness and practice in the workplace?
2. What is the current awareness and practice level of information security among the higher education employees in the Nalut area?

2. Related Works:

Information security is the process of protecting information that has a recognized value; the information is the core of information security that must be protected. The information security involves all the technical, behavioural, managerial and organisational approach to reduce the threats on information assets. The aim of information security is to ensure the Confidentiality, Integrity and Availability (CIA) of information assets of an organisation (Bozic, 2012; Albrechtsen, 2007; Da Veiga et al., 2007).

In the context of the organization, Chan et al., 2005 in their study found a large number of information security breaches in the workplace resulted from employees' failure to comply with organizational information security guidelines. They found that 78% of computer attacks appear in the form of viruses embedded in email attachments. Employees who open email attachments from unknown sources face risk infecting their own computers as well as other computers sharing the same network. Therefore, more attention needs to be paid learning how non-compliant behavior takes place so that appropriate measures for curbing the occurrence of such behavior can be found.

According to Jones et al. (2010), organisations thought that insiders are the essential fraction of the losses of the organisation's information systems, where 69% of the respondents reflected the financial losses to insiders. The majority of the security incidents were caused by unintentional mistakes by employees, the majority of respondents reflected that the security incidents are stemming from misuse of network resources. Consequently, cybercrime activities have increased and end-users find themselves the recipient of threats.

Ishak et al. (2014), conducted a study on information security awareness and practice among faculty staffs in University Selangor Malaysia IHLs, the study found that security awareness and practice level was good among the staff, where, more than half of them were aware of information security issues, however, they usually do not practice secure computing behaviors as such they aware. The study suggests that Malaysian IHLs should develop information security policy to confirm that academic staff can understand their role on information security at their academic institutions, security policies should be focused on security standard, password management, back-up data, comply with good security practice, manage

phishing emails, documents and data storage devices. Other than that training programs are needed to enhance security awareness and practice.

In summarizing the above literature, to ensure that information security could be achieved in any organization, there is a sufficient review of literature to warrant research into the proposed key factors that affect security awareness and practice of employees in the workplace. Several studies on information security awareness and practice presented these factors and their role on the security awareness and practice and their various roles on the information security within an organization. These key factors are: policy, behavior, training, knowledge of technology, and education. The conceptual framework for security awareness and practice. Figure 1 shows the conceptual framework of the factors that influence information security awareness and practices in an organization

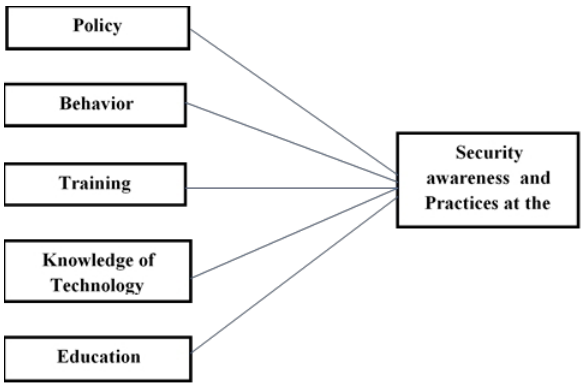

Figure 1: A conceptual framework for the security awareness and practice

3. Methods:

The purpose of this study is to identify and describe the relationship between employee's security awareness and practice, dependent variable and the factors that affect security awareness and practice in the workplace, independent variables

Almost 202 questionnaires collected from Nalut University and Higher Institute of Science and Technology in Nalut, Nalut city located at the western end of the Nafusa Mountains in Libya. The survey used a three-point Likert scale with "1 = No, 2 = Not Sure and 3 = Yes". Section 1 obtained information related to the respondents. Section 2 is obtaining information related to security awareness and practices at the workplace. These questions show the level of information security awareness and practice. Section 3 obtained information related to factors that affect information security awareness and practices at the workplace, these questions aim to find out the relation between the factors that are defined in the conceptual framework of information security awareness and employee's security awareness and practice at the workplace.

4. Findings:

The findings include descriptive analysis, Correlation analysis was conducted to identify the major factors for evaluating information security awareness and practice in the workplace among the higher education employees in the Nalut area.

4.1 Demographic information:

The table below shows the distribution of demographic information, gender, age group, education and job role

Table 1: Frequencies of demographic information

Demographic factor		Frequency	Percent
Gender	Male	89	44.1%
	Female	113	55.9%
Age Group	Below20	3	1.5%
	20-24	18	24.3%
	25-29	49	34.7%
	30-34	70	33%
	35-39	29	14.4%
	40 and above	33	16.3%
Education Level	Certificate	24	11.9%
	Diploma	70	34.7%
	Bachelor	60	29.7%
	Master	43	21.3%
	PhD	5	2.5%
Job Role	Academic	82	40.6%
	Administration	120	59.4%

4.2 Descriptive Analysis:

4.2.1 Security Awareness at the workplace

The results of the descriptive statistics to each item of the security awareness at the workplace are presented in table 2.

Table 2: Descriptive Statistics for Security Awareness

Items	Workplace	
	Mean	±Std. Deviation
I am aware of the vulnerabilities associated with sharing devices.	2.62	.690
I am aware of the encryption that can prevent unauthorized access to confidential information.	2.50	.748
I am aware that it is important to back up my files.	2.64	.686
I am aware that information security is necessary to protect my information.	2.75	.574
I am aware of virus protection software that requires frequent updates.	2.81	.465

Respondents were asked about their security awareness at the workplace by using a Likert scale with "1 = No, 2 = Not Sure and 3 = Yes". Results revealed that the overall mean was 2.66 ± 0.63 for the workplace. The highest mean refers to the statement that they are aware of virus protection software that requires frequent updates for workplace with (2.81) this might be because the virus protection software is common in use for securing computers so the majority of respondents are aware of using such software. The lowest mean refers to the statement they were aware of the encryption that can prevent unauthorized access to confidential information for the workplace with (2.50) this might be due to encryption in the advanced level of security protection procedures.

4.2.2 Security Practice at the workplace

The results of descriptive statistics to each item of security practice at the workplace are presented in table 3.

Table 3: Descriptive Statistics for Security Practice

Items	Workplace	
	Mean	±Std. Deviation
I log off my computer whenever I leave it.	2.67	.649
I regularly backup my data.	2.51	.768
I do not download or install unauthorized copies of software.	2.59	.686
I make sure the antivirus software is enabled and updated.	2.58	.696
I use firewall protection	2.62	.683

Respondents were asked about their security practice at the workplace by using Likert scales of "1 = No, 2 = Not Sure and 3 = Yes". Results revealed that the overall mean was 2.59 ± .69 for the workplace. The highest mean score refers to respondents who log off their computer whenever they leave it with (2.67), comes second with use of firewall protection in workplace mean score (2.62) at workplace, while the users practice of not downloading or installing unauthorized copies of software comes third with (2.59) for workplace. The practice of making sure the antivirus software enabled and updated comes next with mean scores (2.58) for the workplace. The lowest mean score goes to respondents regularly backing their data with (2.51) for workplace, this might be due to that in the workplace backup data is one of the policy and procedures to recover from disaster that could damage the information system.

4.2.3 Policy

The results of descriptive statistics to each item for policy at the workplace and are presented in Table 4.

Table 4: Descriptive Statistics for Policy

Items	Workplace	
	Mean	±Std. Deviation
Team related to security is needed.	2.69	.603
I know who to contact if my computer is hacked or infected.	2.49	.761
My computer is configured to automatically update.	2.54	.699
I have policies on which websites I am allowed to visit.	2.59	.722
There are guidelines regarding information security that I can refer to.	2.56	.697

Respondents were asked about the policy at their workplace by using a three- Likert scale "1 = No, 2 = Not Sure and 3 = Yes". The result revealed that the overall was 2.57 ± .69 for the workplace, the highest mean refers to a team related to security is needed (2.69). The lowest mean refers to knowing who to contact if the users computers are hacked or infected with a mean of 2(2.49), while policies of the allowed websites to be visited came with mean (2.59), while if there are guidelines regarding the information security that they can refer to comes with (2.56) and my computers are configured to automatically update with (2.54)

4.2.4 Behavior factor

The results of the descriptive statistics to each item of the behavior factor at workplace presented in table 5.

Table 5: Descriptive Statistics for Behavior

Items	Workplace	
	Mean	±Std. Deviation
I'll make sure that when I delete a file from the computer or USB stick, that the information is totally removed.	2.70	.617
I feel that my PC is safe.	2.50	.707
I often take information from the office and use a computer at home to work on it.	2.50	.755
I do not share my password.	2.59	.679
I use the same password both for work and home accounts.	2.51	.748

Respondents were asked about their behavior practices in using computers at the workplace by using a three- Likert scale "1 = No, 2 = Not Sure and 3 = Yes". The result revealed that the overall mean was 2.56 ± .70 in the workplace. The highest mean refers to that the users will make sure that the information is totally removed when they delete a file from the computer

or USB stick with a percentage of (2.70) at workplace while if they do not share their password at workplace with (2.59). The lowest mean refers to two statements the users feel that their PCs are safe in the workplace, and they often take information from the office and use a computer at home to work on it with mean (2.50).

4.2.5 Training factor

The results of the descriptive statistics to each item of the training factor are presented in Table 6.

Table 6: Descriptive Statistics for Training Factor

Items	Workplace	
	Mean	±Std. Deviation
I attended a security training course lately.	2.05	.978
I receive adequate information security training.	1.94	.973
Training makes me more aware (increase my awareness).	2.67	.671
Training promotes security awareness.	2.61	.733
Training promotes security practices.	2.64	.686

Respondents were asked about their training by using a three- Likert scale "1 = No, 2 = Not Sure and 3 = Yes". The result revealed that the overall mean was 2.38 ± .80. The highest mean refers to that training makes me more aware with (2.67), if the training promotes security practices comes with (2.64), training promotes security awareness with (2.61) and if the users attended security training course lately with (2.05). The lowest mean refers to if the users receive adequate information security training with (1.94)

4.2.6 Knowledge of IT

The results of descriptive statistics to each item of knowledge of IT at the workplace presented in Table 7.

Table 7: Descriptive statistics for knowledge of IT factor

Items	Workplace	
	Mean	±Std. Deviation
I have installed, updated, and enabled, antivirus software on my computer.	2.62	.703
I know what the risk is when opening emails from unknown senders; especially if there is an attachment.	2.56	.690
I know what an email scam is and how to identify it.	2.46	.779
I know how to use antivirus software and how to scan for viruses.	2.62	.710

Respondents were asked about their knowledge of IT at the workplace by using a three- Likert scale "1 = No, 2 = Not Sure and 3 = Yes". The result revealed that the overall mean was 2.56 ± .72 at the workplace. The highest mean (2.62) for the workplace refers to two statements: the users' knowledge of how to use antivirus software and how to scan for viruses and if the users have installed, updated, or enabled, antivirus software on their computers. The lowest mean score refers to the users' knowledge about what an email scam is and how to identify it with (2.46), this might be due to the fact that the users are not familiar with the threats of an email application.

4.2.7 Education

The results of descriptive statistics to each item of education at the workplace presented in table 8.

Table 8: Descriptive statistics for Education

Items	Workplace	
	Mean	±Std. Deviation
I know what social engineering (phishing) attack is.	2.52	.793
I know what to do if my computer is infected with a virus.	2.52	.721
I never found a virus or a Trojan on my computer.	2.51	.728
My computer has no value to hackers, they do not target me.	2.44	.766
I always download and install software on my computer.	2.63	.657

Respondents were asked about their education at the workplace by using a three- Likert scale "1 = No, 2 = Not Sure and 3 = Yes". The result revealed that the overall mean was 2.52 ±.73. The highest mean goes to the users who are always downloading and installing software on their computers with (2.63). The second mean goes to two statements if they know what social engineering (phishing) attack is, and if they know what to do if their computer is infected with a virus with (2.52). The lowest mean refers to if the users never found a virus or a Trojan on their computer with (2.51), this may be due to the fact that virus threats are common through using the internet.

4.3 Correlation Analysis

In the present study, Pearson Correlation analysis was conducted in order to examine the relationship between the independent variables (policy, behavior, training, knowledge of technology and education) and the dependent variables (security awareness and security practice) in workplace. Correlation analysis is considered a statistical method that is used to describe the strength and direction of the linear relationship between two variables (Pallant, 2013).

The degree of correlation is concerned with measuring the strength and importance of a relationship between the variables. To achieve this, the bivariate association was conducted. The procedure computes Pearson's Correlation coefficient with significant levels. Pearson Correlation coefficients can only take one value which ranges from - 1 to +1. The magnitude of the absolute value by ignoring the sign provides an indication of the strength of the relationship between two variables. Burn (2000) provides a guideline to explain the strength of the relationship between two variables (r) as shown in table 9.

Table 9: Burn Guideline of Correlation Strength

Absolute Value of Correlation Coefficient	Remarks on Correlation (rho)	Nature of Relationship
0.90 - 1.00	Very high correlation	Very strong relationship
0.70 - 0.90	High correlation	Marked relationship
0.40 - 0.70	Moderate correlation	Substantial relationship
0.20 - 0.40	Low correlation	Weak relationship
Less than 0.20	Slight correlation	Relationship so small as to be negligible

Source: Burn (2000).

4.3.1 Independent Variables and Security Awareness at Workplace

Table 10 represents a summary of the relationships between the independent variables (policy, behavior, training, knowledge of technology and education) and the dependent variable (security awareness) in the workplace. In general, the results revealed that there are significant and positive relationships between policy, behavior, training, knowledge of IT and education with security awareness at the workplace. All variables have a moderate positive relationship with security awareness at the workplace except training has small positive relationship as the significant yielded a value of .001 and the correlation value were (R = .346**)

Table 10: Summary of correlations of variables Policy, Behavior, Training, Knowledge of IT, Education and Security Awareness at Workplace (Dependent variable) of the study model

Independent variables	Correlation coefficient	Strength of relationship
Policy	.650**	Moderate
Behavior	.639**	Moderate
Training	.346**	Small
Knowledge of IT	.566**	Moderate
Education	.605**	Moderate

* Correlation is significant at 0.01 level (2-tailed).

4.3.2 Independent variables and Security Practice at Workplace

Table 11 represents a summary of the relationships between the independent variables (policy, behavior, training, knowledge of technology and education) with the dependent variable (security practice) at the

workplace. In general, the results revealed that there are significant moderate relationships between policy, behavior, training, knowledge of IT and education with security practice at the workplace. All variables show a moderate relationship with the security practice at the workplace except training has small positive relationship as the significant yielded a value of .001 and the correlation value were (R = .348**)

Table 11: Summary of Correlations of Variables Policy, Education, Behavior, Knowledge of IT, Training and Security Practice at Workplace (Dependent variable) of the study model

Independent variables	Correlation coefficient ®	Strength of relationship
Policy	.616**	Moderate
Behavior	.601**	Moderate
Training	.348**	Moderate
Knowledge of IT	.532**	Moderate
Education	.569**	Moderate

* Correlation is significant at the 0.01 level (2-tailed).

Information security awareness of employees needs to be constantly developed as security awareness campaigns initiatives and training programs are important to increase the awareness and practice of the users' workplace. Therefore, employees can practice the proper security behavior in their workplace and also increase their IT knowledge rather than remaining ignorant in this area. With respect to the research objectives stated achievements for each objective are discussed below:

Conclusion

Information security awareness and practice required improvement for users so that users become more aware of the necessity to practice good behavior in their daily activity. This paper reviewed the existing knowledge on security awareness and practice and was confined to the key five factors which are; policy, behavior, training, knowledge of IT, and education. The survey instrument was developed to measure the perception of the independent variables and their relationship with the dependent variable. The study findings indicated that only policy, behavior, knowledge of IT and education have positive relationships with security awareness and practice in the workplace. Based on the result of Pearson Correlation analysis, the results indicated that there is a small positive relationship between training and security awareness and practice in the workplace. Overall, respondents have a middle level of security awareness and practice in the workplace. Further investigation is required especially with the training factor. It is suggested that universities should develop security awareness training programs which elevate the employees' awareness and practice in the workplace.

References:

1. Albrechtsen, E. 2007. "A qualitative study of users' view on information security". Computers & security, 26(4), PP. 276-289.
2. Alfawaz, S. Nelson, K. and Mohannak, K. 2010. "Information security culture: A behaviour Compliance Conceptual Framework". Proceedings of the Eighth Australasian Conference on Information Security-Volume 105. Australian Computer Society, Inc. PP. 47-55.
3. Bozic, G. 2012. "The role of a stress model in the development of information security culture". In MIPRO, 2012 Proceedings of the 35th International Convention (pp. 1555-1559). IEEE.
4. Burn, R.B., 2000. "Introduction to research method". Australia: Longman
5. Chan, M., Woon, I., and Kankanhalli, A. 2005. "Perceptions of information security in the workplace: linking information security climate to compliant behaviour". Journal of Information Privacy and Security, 1(3), pp. 18-41.
6. Da Veiga, A. and J. H. Eloff. 2010. "A framework and Assessment Instrument for Information Security Culture". Computers & Security. Vol. 29. pp. 196-207.
7. Da Veiga, A., Martins, N., and Eloff, J. H. 2007. "Information security culture-validation of an assessment instrument". Southern African Business Review, 11(1), pp. 147-166.
8. Hazari, S., Hargrave, W., & Clenney, B. 2008. "An empirical investigation of factors influencing information security behaviour". Journal of Information Privacy and Security, 4(4), pp. 3-20.
9. Ishak, I.S., Ishak, I.S., Abu Hassan, R., Suradi, Z., and Mansor, Z. 2014. "Information Security Awareness and Practices In Malaysian IHLs: A Study at UNISEL". DOI: 10.15224/978-1-63248-034-7-29 Conference: Second Intl. Conf. on Advances in Computing, Electronics and Electrical Technology - CEET 2014, At Kuala Lumpur.
10. Jones, C. M., McCarthy, R. V., Halawi, L., and Mujtaba, B. 2010."Utilizing the technology acceptance model to assess the employee adoption of information systems security measures". Journal of International Technology and Information Management Vol, 19(2). pp. 43-56.
11. Kruger, H. A., Flowerday, S., Drevin, L., & Steyn, T. 2011." An assessment of the role of cultural factors in information security awareness". In Information Security South Africa (ISSA), 2011 .pp. 1-7. IEEE.

12. O'BRIEN, J. E. S. S. I. C. A., Islam, S., Bao, S., Weng, F., Xiong, W., and Ma, A. 2013. "Information security culture: literature review". Department of Computing & Information Systems. University of Melbourne. Working Paper.
13. Pallant, J. (2013). SPSS survival manual. McGraw-Hill Education (UK)
14. Rezgui, Y., and Marks, A. 2008. "Information security awareness in higher education: An exploratory study". Computers & Security, 27 (7), pp.241-253.