



Exploring Libyan Higher Education Institutions Employees' Information Security Policy Awareness

Aisha Aissa Ali Ahmed

Doctor of Philosophy, Faculty of Artificial Intelligence,
Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia

Hafiza Abas

Advanced Informatics Department,
Universiti Teknologi Malaysia,
Kuala Lumpur, Malaysia,

ABSTRACT

Incidents of data breach in higher education could harm students since the exposure of sensitive student data (e.g., social security numbers) could twist students into victims of identity theft and endanger their identities. Regrettably, while most of the developed countries have standard information security laws apply to higher education institutions, such laws are still in its infant stage in developing countries like Libya. However, there are established policies documented by Libyan authorities to guide employees against information security breach, yet existing higher education institutions' information security awareness models did not investigate these policies into the awareness programs. Consequently, employees will rely on policies that can subvert the security best practice. This study aimed to explore the level of understanding of Libyan information security policies among employees of higher education institutions. The quantitative technique is applied in this research, 196 employees of Libyan higher education institutions were randomly surveyed to respond to Linker information security policy awareness questionnaire. Using SPSS statistics tools, a descriptive analysis of the data is achieved. The findings of the study revealed that employees of Libyan higher education institutions are much aware of Internet Usage and Workstation security policies.

Keywords: Awareness, Higher Education, Information Institution, Policy Security.

INTRODUCTION

Employee awareness and compliance with information security policies affect an organization's information asset protection. Internal threats, whether intentional or accidental, pose significant risks in the evolving information security landscape. The literature emphasizes information security awareness as a key risk mitigation strategy. Bulgurcu, Cavusoglu [1], Li, He [2] found that rationality-based beliefs and cybersecurity policy awareness affect employees' security behaviors. This emphasizes the need for information security policies and effective awareness programs to change employee security behavior. Organizational culture greatly affects compliance with information security policy. Wiley, McCormac [3] find that organizational culture affects information security awareness and can improve compliance. According to McIlwraith [4], effective employee education, training, and awareness strategies

reduce information security risks. Due to the dynamic nature of security threats and the complexity of information systems, awareness programs must be updated and aligned with current security standards and practices to be effective.

Despite their benefits, information security awareness programs face implementation and effectiveness issues. According to Bada, Sasse [5], many awareness campaigns fail to change behavior due to a lack of engagement, inappropriate messaging, or a holistic approach that integrates awareness with organizational culture and daily practices. According to Hwang and Cha [6], technostress and role stress can result from the pressures and complexities of following strict security policies. Thus, awareness programs must educate employees about policies and address organizational and psychological factors that affect security behavior to succeed.

The Information is sensitive, interactive, and collaborative, especially in the context of the educational process. One of the most important educational institutions is the higher education institutions that use databases and digital information to support research and academic lessons or even manage the essential activities of the administrative staff [7]. Information in higher education institutions is regarded as a valuable asset in information security policy, which consists of teaching, learning, scientific research, administrative, public service, and cultural data. However, many academics have been concerned about information security as the Internet has grown [8].

Information security means protecting information and information systems from unauthorized access, use, disruption, or destruction [9] or defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction [10]. In the perspective of organization, Chan, Woon [11] revealed a huge number of information security breaches in the workplace resulted from employees' refusal to abide by the organizational information security guidelines. The security of the information remains very important for any organization. Generally, the element of humans in securing information is a considerable reliance in terms of knowledge as well as behavior; which means that protecting information is necessary for those who are engaged in work in this sector to ensure a high level of information security [12]. This is why issues associated with information security were classified as technical problems for years. Users' behavior is affected by awareness as well as the security culture. This is why the factor of humans must pay more attention to providing information protection Alfawaz, Nelson [13], Lima, Kim [14]. However, most cyber-attacks and threats target data from higher education institution (HIE) [14].

Due to the lack of data security, hacking into information systems is becoming increasingly common in the education sector. Thus, to support the organization's objectives in securing information, it follows specific procedures and security standards as well as regulations [15]. Hackers easily bypass security mechanisms to attack universities and colleges for two reasons: Firstly, providing open access by the universities for students and guests. Staff and employees' role in protecting the information inside their organization is the second reason [16]. Implementing information security model presents issues and challenges, especially in developing countries [17]. The Libyan higher education institution (LHEI) system is one of the sectors viewed as vital for the country's redevelopment [18]. Hence, many LHEIs have already acknowledged the impact of adopting the information security model paradigm to enhance the

security model and teaching processes. This has called for more research concerning the information security model paradigm to promote its general use Ramadan, Elatresh [18], Othman, Pislaru [19], Salem and Mohammadzadeh [20]. Consequently, this paper will explore the understanding of information security policies established by Libyan authorities among the employees of higher education institutions. Based on the research gaps, the study offers a research question:

- How effective are information security awareness programs in Libyan higher education institutions (LHEIs) in changing the security behaviors of employees and students?

LITERATURE REVIEW

Employees' Information Security Policy Awareness

An extensive literature review emphasizes the importance of awareness and organizational context in employee compliance with information security policies. Bulgurcu, Cavusoglu [1] noted that policy compliance depends on employee beliefs aligning with organizational security goals. Li, He [2] found that employee cybersecurity behavior improves with cybersecurity policy awareness and understanding. Khando, Gao [21] explain how targeted awareness programs can fill gaps in employee knowledge and behavior, improving an organization's security. Bada, Sasse [5] found that implementing these programs takes time and effort. These researchers argue that many awareness campaigns fail because they fail to engage employees and overlook security practices' real-world applications and implications. Hwang and Cha [6] argue that technostress and role stress cause non-compliance and that awareness programs should reduce these stressors to improve security protocol compliance.

Another key finding from the literature is that security awareness strategies must incorporate organizational culture. Wiley, McCormac [3] claim that organizational culture greatly affects security awareness programs. D'Arcy and Lowry [22] show that cognitive-affective factors like employee attitudes and emotions toward security policies shape compliance behaviors over time. McIlwraith [4] agrees that continuous education and training promote a proactive security culture. The development and deployment of information security awareness initiatives must be strategic. Moody, Siponen [23] propose an integrated model for information security policy compliance that integrates organizational, technical, and psychological factors, advocating for multifaceted security education. According to Steinbart, Raschke [24], a positive relationship between internal audit and information security functions improves security outcomes, emphasizing the need for collaborative and integrated strategies in organizations.

Employees' Information Security Policy Awareness in Higher Educational Institution (HEI)

According to Gharieb [25], there are security awareness of users in educational institutions so that users can reduce the occurrence of insecure times such as information leakage in terms of their own use. Higher education institutions contains sensitive data that lead to them being at higher risk [26]. Expert in computer security have agreed that universities are among the least information security secured environment (Lund, 2018). According to Abdallah, Abdalla [27] literature shows that the development of information security remains uncertain and a complicated process to protect personal and vulnerable information from cyber-attack. Also, Information security awareness is often overlooked in information security programs [28]. As at 2007, marks highlighted that the number of scientific studies that consider Information

Security awareness in developed countries, especially in higher education environment is very limited. As such, researchers strive ways of studying information security awareness on organizations and institutions of higher education to ensure employees, users and data custodian are conversant with information security models and paradigms.

Schütz, Weber [29] examined information security awareness of students at a German University, the analysis results highlight the need for awareness in the areas of changing initial passwords, not using USB drives, knowledge about anti-virus systems, and reporting security incidents. Other scholars have studied the security awareness of users in educational institutions so that users can minimize the occurrence of insecure times such as information leakage in terms of their own use [25]. Besides, [30] stressed the need for universities to engage students into information security awareness training while previous studies found that only a few universities give information security awareness training to students [31].

The awareness of information security helps in minimizing the risks to information assets. Especially, when the risk of unwise behavior is reduced from the employee and harmful interaction with information. However, with the advancement of globalization and its effect, organizations are indeed applying information security awareness, along with implementing a strong information security background [4]. Therefore, the employees themselves can cause risk to information security assets due to the weakness of practices as well as unawareness of information threats [32]. The home users, employees of organizations have to comply with the policies and roles of their organization to safeguards and protect the information using firewalls and antivirus programs [33]. While safeguarding and protecting information among home users and employees are generally emphasized, very few resources are used to increase the overall security awareness of users. Thus, making them the weakest link in the organization [34]. Focusing on Libya, Tamtam and Asker [16] proposed a conceptual framework for security awareness and practice, the model centered on examining the various factors that can influence or affect users' practices and awareness at home. Nevertheless, the model has not taken into consideration the security awareness of higher education in Libya. Higher education has become a profitable target for cyber-attacks, this mandate many institutions reevaluating their cybersecurity awareness programs [28].

With advances in technology and concepts, many developed countries, including the United States, are making efforts to strengthen public awareness of information security and are urging university leaders to take appropriate measures to protect the university's information network [35]. Also, EU adopted the General Data Protection Regulation in 2016, which has had a global impact and can be applied to institutions that process student data as well as third-party service providers to provide clear regulation of their data operations, organizations are required to collect and use personal data lawfully and to provide appropriate privacy protections [36]. However, studies have shown that the development of information security awareness may face more obstacles in developing countries, and the lack of socio-cultural environment and resources, and knowledge may create a gap between the development of this area and developed countries [37]. Also, importance of information security was seriously emphasized by Wiley, McCormac [3], Hadlington, Binder [38], hence, for developing nation like Libya there is need to minimize this gap by embarking on information security awareness programs in universities and other higher education institutions. Efforts have been made to

study information security and practice among faculty staffs in University Selangor Malaysia [39], in United Arab Emirate (UAE) similarly, Abdallah, Abdalla [27], explored information security awareness among higher education students and examined the key variables that influenced its behavior. Tamtam and Asker [16] investigate the factors that may impact users' practice and awareness in workplace with emphasize on third level education, Nalut Libya as a case study, the findings indicated that only policy, behavior, knowledge of IT and education have positive relationships with security awareness and practice in the workplace.

Although the development of a comprehensive information security laws are still in its infant stage in developing nations, Libyan authority have documented information security policies for organization and government employees to improve their security best practice [40]. Nevertheless, existing information security awareness models of Libyan higher education institutions are yet to incorporate these policies into their awareness programs, rendering students and employees in the former system of security practice. However, in countries like China, the level of information security awareness among Chinese college students revealed that students have some awareness of information security and can take some basic precautions, but their personal practices are not sufficient, with a significant lack of security awareness in file sharing and password security, and a lack of personal awareness of the risks of cyberattacks [41]. Overall, researchers have proposed various models of information security awareness, but there is currently lack of attention and research on information security policy awareness model of Libyan higher education institution with focus on the established information security policies established by National Information Security & Safety Authority [40, 42].

METHOD

Research Design

The purpose of this study was to explore employees' awareness information security policies established by National Information Security and Safety Authority, Libya in their respective higher education institutions. A quantitative research method was selected for this research. This is because its purpose is to ask narrow objective questions and generate quantitative data that can be analyzed using statistics [36, 43-48].

Target Participants

The research used a quantitative method. Employees' awareness information security policies were considered as a variable that could be measured by a questionnaire. A convenience sampling technique was used in this study and 196 employees from different higher education institutions across different regions of Libya participated in this questionnaire. The questionnaire was distributed online to conduct the survey and it was carried out in 21st May to August 2023. Taking ethical considerations into account, an information sheet was appended before completing the questionnaire to explain the main purpose of the survey and to seek employees' permission to participate in the study. The participation was voluntary and anonymous and withdrawal from the study was possible at any time.

Instruments and Procedures

In this paper, a questionnaire was dispersed to investigate the information security policy awareness of university employees. The questionnaire was structured into two parts, the first part was demographic information including the age and gender of the participants. The second

part was questions related to the participants' information security policy awareness. The questionnaire in this study was designed using the information security policies established by National Information Security & Safety Authority [40]. And the number of items in the questionnaire will be 15, the items were tested on employees using a Linkert-type 5-point scale ranging from strongly disagree (1) to strongly agree (5) and supply as answer possibilities for all items. Data was collected and then analyzed using descriptive statistics. The 15 questions were extracted from password, email usage, Internet usage and workstation security policies [40] and presented as follows:

Password Policy:

Strong password policies are essential to any organization's cybersecurity [24, 49]. A mix of uppercase, lowercase, numbers, and symbols, along with a minimum length, is usually required for strong passwords to prevent brute force or dictionary attacks. Complex passwords make user accounts more secure by making them harder to guess or crack. Implementing policies that require users to change their initial passwords and regularly update them, (forcing expiration) is also important [50]. This reduces the risks of password aging, such as unauthorized access from unchanged, compromised credentials. Frequent updates limit a cyberattacker's ability to exploit a compromised password.

Password storage security is also crucial. Organizations must use industry-standard encryption to secure passwords [51, 52]. This prevents plaintext password storage, a major vulnerability. Encrypting passwords prevents data theft and security breaches by safeguarding them with the decryption key. Training and requiring employees to keep their passwords confidential and not share them with coworkers or supervisors is also important. When implemented properly, such measures provide a comprehensive security posture that protects against external and internal threats. When integrated into an organization's information security framework, these policies provide essential digital workplace protections. It includes:

- Require strong password enforcement,
- Require password to be stored in a secure manner,
- Require password to be keep confidential,
- Require changing initial passwords and force expiration,

Email Usage:

- Require every employee to have organizational email account,
- Require approval before signing into social media website,
- Require users to be aware that emails may be subject to audit.

Internet Usage:

- Require that user internet access requirement will be periodically reviewed.
- Require IT technical support to download software upgrades and patches
- Require not to use organization internet to cause damage to the organization network.
- Require User to be fully responsible for his/her computer devices and the use of them, and him /her forbidden impersonation of others or devices.

Workstation Security Policy:

- Users should not attempt to access to unauthorized parts of the network,

- Personal privacy and the rights of others should be respected, and should not attempt to obtain data from other users, as well as other programs or files without prior permission
- Require that IT staff should not login into user's devices for maintenance work unless permission is taken directly from the concerned user.

Reliability and Validity of the Approach

Reliability signifies the precision of measurement, this study investigates the reliability of the study based on Cronbach alpha coefficient method as it was rightly used in the previous work [35, 53-57]. The reliability of the questionnaire used in this paper was 0.965 that shows the questionnaire has high reliability and is appropriate for distribution to the respondents.

Similarly, using SPSS version 23.0, the validity of the study was evaluated, Kaiser-Meyer-Olkin (KMO) and Bartlett Coefficient test of the sample data using factor analysis showed a result of 0.919 that indicates the high validity of measurement model.

Data Analysis

To analyze the data, a descriptive analysis of the results using SPSS version 23 was used to generate mean and standard deviation scores, to determine the level of employee's information security policy awareness. Based on the 15 questions submitted, the information concentration was initially explored using factor analysis. Table 1 shows KMO measure of sampling adequacy of 0.919 and Bartlett's test of Sphericity with an approximate Chi-Square of 3381.984 with 105 degrees of freedom and a Sig. of.000. The KMO value is well above the commonly accepted threshold of 0.6, indicating that the sample size is suitable for factor analysis. Field [58] calls KMO values above 0.9 "superb." The data is suitable for structure detection because Bartlett's Test significance level is less than 0.05, indicating population correlation. To prove sphericity, Hair, Black [59], Jandab, Ali [60] recommend factor analysis with zero significance. Thus, these statistical tests demonstrate that the data is suitable for factor analysis because they meet the literature's statistical thresholds (see Table 1).

Table 1: KMO and Bartlett's Test.

<i>Kaiser-Meyer-Olkin Measure of Sampling Adequacy</i>		.919
<i>Bartlett's Test of Sphericity</i>	Approx. Chi-Square	3381.984
	df	105
	Sig.	.000

RESULTS

This section discussed the results of the study and will center on the analysis of the questionnaires generated using descriptive statistics. As highlighted, the first part of the questionnaire focuses on demographic information and the result is shown in Table 2.

Table 2: Gender

Gender	N	%
Male	77	39.3
Female	119	60.7
Total	196	100

Based on the gender of demographic information, 119 (60.7%) of the participants were female and 77 (39.3%) were male. In terms of age composition of the employee, 11(5.6%) were between 18-25, 33 (16.8%) were 26-35, 83(42.3%) were 36-45, and 69 (35.2%) were 46-50 and in terms of education levels 8(4.1%) were secondary, 22(11.2%) were graduate, 75(38.3%) were postgraduate, 74(37.8 %) were professional qualification holders and 17 (8.7%) had other qualifications participated in this questionnaire(As shown in Table 3 and Table 4 respectively).

Table 3: Age

Age	N	%
18-25 Years	11	5.6
26-35 Years	33	16.8
36-45 Years	83	42.3
46-50 Years	69	35.2
Total	196	100.0

Table 4 shows the highest qualifications of 196 people. With 38.3% postgraduates and 37.8% professional certifications, most respondents have higher education. 11.2% are graduates, while 4.1% are secondary school graduates. 8.7% of participants are 'others', which may include vocational training or non-standard education. The data suggests a highly educated sample, with a large representation of postgraduate and professionally certified individuals, suggesting a focus on advanced education and specialized skills.

Table 4: Highest Qualifications

Qualifications	N	%
Secondary	8	4.1
Graduate	22	11.2
Postgraduate	75	38.3
Professional Certification	74	37.8
Others	17	8.7
Total	196	100.0

In addition, Table 5 shows the means and standard deviations of the four dimensions of NISSA, [34] information security policies towards understanding of the employees in Libyan higher education institutions.

Table 5: Mean and Standard deviation.

Dimensions	Mean	Std. Deviation
Password policy	4.777	0.5282
Email Usage policy	4.787	0.5408
Internet Usage policy	4.803	0.4861
Workstation Security policy	4.811	0.5017

The first dimension is password policy with an average score of 4.777 that is a relatively high score. However, when compare with the remaining dimensions it is relatively low, in fact one of the questions about strong password enforcement with 147 (75%) of employees understanding the need of strong password enforcement, indicating that many employees are

still not familiar with the importance of strong password in protecting institutions' information system. In similar trend, the findings of Wang [41] showed that password policy was among the lowest scores in information security awareness among Chinese colleges' students.

In the second dimension, the mean score of Email Usage Policy is 4.787, a bit higher than the password policy. In this dimension, 163 employees out of 196 constitute about 83.2% understand the need for organizational email account. This shows a significant number of employees are aware of email usage policy; this may be because most higher education institutions employees are creating their emails based on the institution websites.

The highest scoring dimensions are Internet Usage and Workstation security with mean scores of 4.803 and 4.811 respectively. One of the highest scoring items was user to be fully responsible for his/her computer devices and the use of them, and he/she has to be aware of the security and preserve of IT resources, out of 196 respondents, 166 out of 196 employees understand this item. Consequently, employees can protect their system from unauthorized access which is vital aspect of information security awareness. Other items that are highly aware by the employees are Personal privacy and the rights of others should be respected, and shouldn't attempt to obtain data from other users, as well as other programs or files without prior permission, next is IT staff should not login into user's devices for maintenance work unless the permission is taken directly from the concerned user and finally forbidden impersonation of others or devices. The aforementioned items scored 165 out of 196 constitute 84.2% of the respondents; these results are highly impressive because it can enhance the privacy of students and employees in Libya higher education institutions.

Based on this study, employees in Libyan higher education institution have shown a great level of awareness in Internet Usage and Workstation security policies, more need to be study in password and email policies. Although previous work of Asker and Tamtam [61] have shown positive awareness of Libyan employees in information security policy, the study is generic and have not specifically addressed the issues in accordance with the National Information Security & Safety Authority (NISSA, 2013) established policies.

DISCUSSION

The research found high compliance with information security policies, including password, email, and internet usage policies. This supports previous studies on the importance of strong policy frameworks and awareness in higher education and corporate settings. Hina and Dominic [7] stressed that well-implemented information security policies improve organizational security in higher education. The high mean scores in our study indicate effective policy implementation and adherence. High compliance rates often indicate a strong organizational security culture, according to the literature. Höne and Eloff [8] discuss how international standards shape effective security policies, suggesting that aligning organizational policies with these standards may explain this study's high compliance levels. Singh, Vaish [9] found that comprehensive information security practices work, and the minimal standard deviation across the surveyed policies suggests that employees understand and implement them.

The consistency in high adherence rates across security policies indicates the effectiveness of organizational training and awareness programs. In organizations that prioritized security

education and awareness, Alhassan and Adjei-Quaye [10] found similar results. This suggests that the policies are strong and supported by ongoing education to ensure compliance. The findings show uniformly high compliance, but Chan, Woon [11] found that policy areas vary, usually due to employee perceptions of relevance. The lack of variation may indicate a well-integrated security culture or that our measurement tools are not sensitive enough to detect finer compliance levels across policy areas.

Finally, Alfawaz, Nelson [13] argue that organizational culture influences compliance. The high compliance rates and the literature's strong, positive security culture show that these outcomes require a multifaceted approach. This includes creating and implementing clear policies and creating an organizational environment that supports and reinforces them through formal mechanisms and cultural norms.

CONCLUSION

Higher education institutions contain sensitive data that lead to them being at higher risk, however, Literature shows that the development of information security remains uncertain and a complicated process to protect personal and vulnerable information from cyber-attack. Also, Information security awareness is often overlooked in information security programs, studies have shown that the development of information security awareness may face more obstacles in developing countries, and the lack of socio-cultural environment and resources, and knowledge may create a gap between the development of this area and developed countries. Consequently, this study strives to analyze the existing approaches in information security awareness in Libya and explore the information security awareness policies of employees of higher education institutions. The findings of the study revealed that employees of Libyan higher education institutions are much aware of Internet Usage and Workstation security policies, nevertheless, more is needed in the aspect of password and email security policies. To complement the effort of this study, future work will include factor analysis to align the study with security best practice and international standard.

References

1. Bulgurcu, B., H. Cavusoglu, and I. Benbasat, Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, 2010. 34: p. 523-548.
2. Li, L., et al., Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 2019. 45: p. 13-24.
3. Wiley, A., A. McCormac, and D. Calic, More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security*, 2020. 88: p. 101640.
4. McIlwraith, A., Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness. 2021.
5. Bada, M., A.M. Sasse, and J.R. Nurse, Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*, 2019.
6. Hwang, I. and O. Cha, Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior*, 2018. 81: p. 282-293.
7. Hina, S. and P.D.D. Dominic, Information security policies' compliance: a perspective for higher education institutions. *Journal of Computer Information Systems*, 2020. 60(3): p. 201-211.

8. Höne, K. and J.H.P. Eloff, Information security policy — what do international information security standards say? *Computers & Security*, 2002. 21(5): p. 402-409.
9. Singh, A., A. Vaish, and P.K. Keserwani, Information security: Components and techniques. *International Journal of Advanced Research in Computer Science and Software Engineering*, 2014. 4(1).
10. Alhassan, M.M. and A. Adjei-Quaye, Information security in an organization. *International Journal of Computer (IJC)*, 2017. 24(1): p. 100-116.
11. Chan, M., I. Woon, and A. Kankanhalli, Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior. *Journal of Information Privacy and Security*, 2005. 1(3): p. 18-41.
12. Kruger, H., L. Drevin, and T. Steyn, A vocabulary test to assess information security awareness. *Information Management & Computer Security*, 2010. 18(5): p. 316-327.
13. Alfawaz, S., K. Nelson, and K. Mohannak. Information security culture: a behaviour compliance conceptual framework. in *Proceedings of the 8th Australasian Information Security Conference (AISC 2010)*. 2010. University of Southern Queensland.
14. Lima, G., et al., Collecting the Public Perception of AI and Robot Rights. *Proc. ACM Hum.-Comput. Interact.*, 2020. 4(CSCW2): p. Article 135.
15. Angraini, R.A. Alias, and Okfalisa. Affecting Factors in Information Security Policy Compliance: Combine Organisational Factors and User Habits. in *Innovative Systems for Intelligent Health Informatics*. 2021. Cham: Springer International Publishing.
16. Tamtam, A. and H. Asker, An investigation of the information security awareness and practices among third level education staff, case study in Nalut Libya. *An Investigation of the Information Security Awareness and Practices among Third Level Education Staff, Case Study in Nalut Libya*, 2020. 16(15): p. 20-32.
17. Ghawail, E.A.A., S.B. Yahia, and M.A. Alrshah, Challenges of applying E-learning in the Libyan higher education system. *arXiv preprint arXiv:2102.08545*, 2021.
18. Ramadan, K., et al., An analysis of factors affecting learners' attitudes towards the integration of e-learning into the higher education system in Libya: Case study; Misurata University. *Australian Journal of Basic and Applied Sciences*, 2019. 13(10): p. 55-64.
19. Othman, A., et al., Analysing the effectiveness of IT strategy in Libyan higher education institutes. *International Journal of Digital Information and Wireless Communications (IJDIWC)*, 2013. 3(3): p. 114-129.
20. Salem, N. and B. Mohammadzadeh, A Study on the Integration of ICT by EFL Teachers in Libya. *Eurasia Journal of Mathematics, Science and Technology Education*, 2018. 14(7): p. 2787-2801.
21. Khando, K., et al., Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & security*, 2021. 106: p. 102267.
22. D'Arcy, J. and P.B. Lowry, Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, 2019. 29(1): p. 43-69.
23. Moody, G.D., M. Siponen, and S. Pahnla, Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly*, 2018. 42(1): p. 285-A22.

24. Steinbart, P.J., et al., The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society*, 2018. 71: p. 15-29.
25. Gharieb, M.E., Knowing the level of information security awareness in the usage of social media among female secondary school students in Eastern Makkah Al-Mukarramah-Saudi Arabia. *International journal of computer science and network security: IJCSNS*, 2021. 21(8): p. 360-368.
26. Yerby, J. and K. Floyd. Faculty and staff information security awareness and behaviors. in *Journal of The Colloquium for Information Systems Security Education*. 2018.
27. Abdallah, N., et al., Information security awareness behavior among higher education students: Case study. *Journal of Theoretical and Applied Information Technology*, 2020. 8(10): p. 3825-3836.
28. Hobbs, J., Cybersecurity awareness in higher education: a comparative analysis of faculty and staff. *Issues in Information Systems*, 2023. 24(1).
29. Schütz, A.E., K. Weber, and T. Fertig, Assessing the Information Security Awareness of University Students. 2020.
30. Kim, E.B., Recommendations for information security awareness training for college students. *Information Management & Computer Security*, 2014. 22(1): p. 115-126.
31. North, M.M., R. George, and S.M. North, Computer security and ethics awareness in university environments: a challenge for management of information systems, in *Proceedings of the 44th annual Southeast regional conference*. 2006, Association for Computing Machinery: Melbourne, Florida. p. 434-439.
32. Da Veiga, A. and J.H.P. Eloff, A framework and assessment instrument for information security culture. *Computers & Security*, 2010. 29(2): p. 196-207.
33. Nasir, A., M. Rashid, and A. Hamid. Conceptualizing and validating information security culture as a multidimensional second-order formative construct. in *The Thirteenth International Multi-Conference on Computing in the Global Information Technology*. 2018.
34. Aloul, F.A., The need for effective information security awareness. *Journal of advances in information technology*, 2012. 3(3): p. 176-183.
35. Roach, R., Ringing the alarm on campus computer security. *Diverse Issues in Higher Education*, 2001. 18(20): p. 50.
36. Steiner, C.M., M.D. Kickmeier-Rust, and D. Albert, Let's talk ethics: Privacy and data protection framework for a learning analytics toolbox. *Ethics and Privacy in Learning Analytics (# EP4LA)*, Poughkeepsie, NY, 2015.
37. Rezgui, Y. and A. Marks, Information security awareness in higher education: An exploratory study. *Computers & Security*, 2008. 27(7): p. 241-253.
38. Hadlington, L., J. Binder, and N. Stanulewicz, Exploring role of moral disengagement and counterproductive work behaviours in information security awareness. *Computers in Human Behavior*, 2021. 114: p. 106557.
39. Ishak, I., et al., Information Security Awareness and Practices In Malaysian IHLs: A Study at UNISEL. DOI, 2014. 10: p. 978-1.
40. Sherif, E., Information security policy: The national payment system in Libya. 2012.

41. Wang, X., Exploring Chinese college students' awareness of information security in the COVID-19 era. *European Journal of Education*, 2022. 5(2): p. 19-33.
42. Weippl, E.R. and M. Ebner. Security privacy challenges in e-learning 2.0. in *E-Learn: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education*. 2008. Association for the Advancement of Computing in Education (AACE).
43. Abdulhadi, A.R., et al., The Impact of Risk Management on The Dimensions of Project Management Among Small and Medium Enterprises in Iraq. *Advances in Social Sciences Research Journal*, 2022. 9(11).
44. Abdulsamad, A., et al., The Importance of Entrepreneurial Orientation's Dimensions in Influencing the Organizational Performance of Food and Beverage SMEs. *Advances in Social Sciences Research Journal*, 2020. 7(12).
45. Al-Sharif, A.M., et al., The Role of Innovation Capability in the Relationship between Entrepreneurial Leadership and Innovation Performance in the SMEs Service Industry. *Advances in Social Sciences Research Journal*, 2023. 10(1).
46. Al-Zubaidi, R., et al., Sustainable Development Through Effective Project Management: The Petromasila in Yemen. *Advances in Social Sciences Research Journal*, 2023. 10(3).
47. Alghamdi, M.A.A., et al., Antecedents and Consequences of Employee Well-Being: Empirical Study on Saudi Aramco. *Advances in Social Sciences Research Journal*, 2021. 8(9).
48. Jandab, A., et al., THE INFLUENCE OF IT CAPABILITY ON IT-BASED INNOVATION: THE MEDIATING ROLE OF ORGANIZATIONAL LEARNING CAPABILITY. 2020: p. 2020.
49. Aldawood, H. and G. Skinner. Educating and raising awareness on cyber security social engineering: A literature review. in *2018 IEEE international conference on teaching, assessment, and learning for engineering (TALE)*. 2018. IEEE.
50. Kuppusamy, P., et al. Systematic literature review of information security compliance behaviour theories. in *Journal of physics: conference series*. 2020. Institute of Physics Publishing (IOP Publishing).
51. Mughal, A.A., Artificial Intelligence in Information Security: Exploring the Advantages, Challenges, and Future Directions. *Journal of Artificial Intelligence and Machine Learning in Management*, 2018. 2(1): p. 22-34.
52. Zeng, E. and F. Roesner. Understanding and improving security and privacy in {multi-user} smart homes: A design exploration and {in-home} user study. in *28th USENIX Security Symposium (USENIX Security 19)*. 2019.
53. Abdulhadi, A.R., et al., The Impact of Internal Control on Project Management in Construction Site Among Small and Medium Enterprises in Iraq. *Advances in Social Sciences Research Journal*, 2023. 10(3).
54. Abdulsamad, A., et al., The Importance of Entrepreneurial Orientation's Dimensions in Influencing the Organizational Performance of Food and Beverage SMEs. *Advances in Social Sciences Research Journal*, 2020. 7: p. 81-99.
55. Al-Sharif, A., et al., Effects of Innovation Capability and Environmental Dynamism on the Relationship between Entrepreneurial Leadership and Innovation Performance in the SMEs Service Industry. *International Journal of Academic Research in Business and Social Sciences*, 2023. 13: p. 1547-1570.
56. Al-Zubaidi, R., et al., The Effect of Self-efficacy on Sustainable Development: The PetroMasila in Yemen. *Advances in Social Sciences Research Journal*, 2022. 9: p. 35-49.

57. Alghamdi, M.A.A., et al., Employee Well Being and Knowledge Sharing Behavior Among Employees of Saudi Aramco. *Advances in Social Sciences Research Journal*, 2021. 8(8).
58. Field, A., *Discovering statistics using IBM SPSS statistics*. 4th ed. 2013: sage. 952.
59. Hair, J.F., et al., *Multivariate data analysis*, ed. t. ed. 2010, Uppersaddle River, New Jersey: Pearson Education International.
60. Jandab, A., et al., IT-Based Innovation and New Product Development Performance in Yemen: The Moderating Role of Intellectual Property. *International Journal of Business Society*, 2019. 3(11): p. 1-8.
61. Asker, H. and A. Tamtam, Knowledge of information security awareness and practices for home users: Case study in Libya. *ESI Preprints*, 2023. 14: p. 22-22.