Investigating Practices of Information Security Awareness: Perspectives from Government Entities in Libya

Almabruk Sultan
University of Benghazi
Computer Science Dept.

Elmabruk Laias
University of Benghazi
Computer Science Dept.

Ahmed El Saiti
Aljeel Aljadeed For Technology
Benghazi, Libya

ABSTRACT
Government and military organizations and other organizations process and store huge volumes of confidential data, regularly transmitted across networks, thereby increasing their exposure to security threats. The probable damages can lead to monetary losses and put national security at risk if critical information infrastructure is targeted. This study examined the level of information security awareness (ISA) and information security (InfoSec) practices in all departments among the general public (non-IT departments) in Libyan organizations. This examination was conducted using an online and manual survey that was based on instruments produced by organizations specializing in information security (InfoSec), due to cultural constraints, it would ordinarily be difficult to gather data from female respondents in Libya, however, the use of an online survey helped to collect the data successfully. The ISA survey involved 421 respondents from all department's employees. Results indicated that Libyan organizations' information security awareness (ISA) and practices are quite low. Several areas of weakness in InfoSec appear to be related to the information security standards policies and practices.

General Terms
Security awareness.

Keywords
Information security, Information security awareness, Information security policy, Information security practices.

1. INTRODUCTION
The development that takes place in internet and computer networking technology has consequently led to security challenges as evident in the increase of information threats. This development has undoubtedly necessitated new security procedures and policies to decrease the intensity of the threat and the challenges being encountered from the emergence of the new technology [1]. It is noticed that the new technology is very easy to adopt and adapt to, but some organizations do forget to put a security measure in place to preserve the organization's information from being tampered with. Information Integrity is essential and this is about trustworthiness, origin, completeness, and correction of information, with due obstruction of unauthorized modification of information [2]. To allow information security practices to become routine, there must be an appropriate level of Information Security Awareness (ISA). Information security awareness is a continuous effort to raise attention to information security and its value, to stimulate security-oriented behaviors. Despite the increasing interest of researchers on the topic and the continuous notifications of global security surveys for its big significance, awareness remains a critical issue of information security. In the enterprise environment, security awareness refers to the knowledge and attitude employees possess regarding the protection of the physical and information assets of the organization they work for. Security awareness is a key link in an organization's security chain. Even the most efficient security mechanisms have little value in an organization if there is no security culture to mitigate potential threats, risks, and vulnerabilities. Thus, information users need to have good information security practices because InfoSec is the protection of information and systems and hardware that use store, and transmit that information. These practices are concerned with ensuring the confidentiality, integrity, safety, and of availability information [3]. This study aims to understand ISA and InfoSec practices in Libyan organizations.

2. BACKGROUND OF THE STUDY
Information is now regarded as a valuable commodity if not a vital commodity and however always under constant threat. Information threats can be broadly categorized as natural disasters or human attacks, such as virus attacks, hacking or other intrusions, identity theft, and denial of service (DoS) attacks [4]. The risks and disasters can be mitigated by taking backup and storing redundant copies of information in widely dispersed locations so that the risk of all copies being destroyed or damaged is incredibly low. It is the organized attacks that pose the greatest risk because these attacks are intentional and the mechanisms for conducting such attacks become more sophisticated every day. A computer virus is a type of malicious software, that distributions between computers and causes damage to data, files, and software. Computer viruses target to disrupt systems, result in data loss and leakage, and cause major operational issues. Hackers depend on people leaving computers with inadequate passwords. A Denial-of-Service (DoS) attack is an attack meant to shut down a network, making it inaccessible to its intended users. DoS attacks achieve this by flooding the target with huge traffic or sending it information that triggers a crash. In both instances, the DoS attack denies legitimate users (i.e., employees, members, or account holders) of the service or resource they expected. To decrease the incidence and severity of attacks, it is necessary to raise and increase the level of ISA within a specific organization or in the general public. Information Security policies and practices are usual in most organizations and seek to give employees clear guidelines on what they should or should not do to ensure the security of corporate information. The general public, too, is becoming more aware of several information security risks. However, that is not the case throughout the world. In 2022, the Kaspersky Lab, a highly-respected Information Security specialist, reported the following statistics about the ten targeted countries around the world that had Information

Security attacks. Table 1 represents the known information attacks by country in 2022. To understand these statistics, it must be realized that the number of attacks, to some extent, depends on the number of people using computers and the Internet. Thus, Sudan has more than double the attacks that Uzbekistan does, even though they have similar populations. However, Egypt has nearly double the rate of Internet use that Azerbaijan does, and so more attacks. Once the rate of computer/Internet use is considered, this paper focuses only on the reasons that Libya is so prone to information attacks. Libya has around 6,658,900 computer users in 2021 and around 3,500,000 users in 2008. Libya received 5% of the attacks in 2019. So, Libya accounts for only 0.003 % of the internet users in the world, which is far less than the percentage of attacks they experienced. In 2020 Libya had nearly the same percentage of attacks 4.9% which prompts questioning regarding the reasons for this [5]. Kaspersky, one of the leading companies that specialize in information security, reported statistics about information security and targeted attacks around the world [6].

Table 1: Statistics about the 10 targeted with Security attacks countries around the world (Kaspersky Lab 2022).

No	Country	Percentage of attack %
1	Turkmenistan	6.7%
2	Afghanistan	6.3%
3	Tajikistan	5.2%
4	Yemen	3.7%
5	Uzbekistan	3.5%
6	China	3.3%
7	Mauritania	3.0%
8	Sudan	2.7%
9	Egypt	2.6%
10	Azerbaijan	2.6%

3. RELATED WORK

Cox et al. (2012) claim that security builds requirements of both technology and users. According to Cox et al., secure information needs sound technical solutions, but human behavior is equally important. Therefore, users must understand IS security issues and organizations must help their employees to understand IS security issues [7]. (Aloul, 2012) recommended that Applying awareness training programs will never resolve the purpose. The educational foundation must be tested and held accountable to ensure information security policies and procedures are understood and followed by their entities. information security awareness (ISA) should be developed and there is an instant need for security standards, policies, reporting mechanisms, and continuous awareness training in the educational organizations of UEA [3]. Alotaibi and Alfehaid (2018) proposed that employees must have a suitable level of awareness of the importance of information security (InfoSec) and policies and how to protect themselves against increased threats. Technology solutions alone cannot provide complete protection. Therefore, employees' being aware of security requirements plays a supplementary role in the protection process. understand the issues that surround effective information security awareness (ISA) Applying effective information security awareness (ISA) programs can be a challenging task the human factor is still the weakest link in the information security chain, while there is a movement and an increase in the number of security threats. Using persuasive technology will help in the enhancement of such awareness programs Targeted awareness raising for employees who need increased awareness of a particular issue is one example of the use of persuasive technology [4]. Bhushan (2012) revealed that awareness of information security in India is abysmally low and thus gained a reputation as a country where foreign investors can do business in information security (InfoSec) and have been investing heavily, and explained that the enterprises must put the awareness of employees in their top important to keep on their reputation and mitigate from risks [10]. Jamil and Khan (2011) compared the awareness in India with that of European countries, the concluded that European awareness is better than the Indian awareness. There is not much awareness regarding protecting the data and using them. There is a continuous rise in cybercrime as there is a huge population but fewer resources to manage the population and the cybercrimes that take place and they agree that therefore vital to highlight and support the information security awareness (ISA) in India to improve the infrastructure of information technology [11]. Pandey (2012) concluded that a lack of security awareness was a big gap for cybercriminals. There has been a steady increase in the number of cybercrimes as people are not aware of the rapid developments in the cyber world. The study also concluded that the absence of experts and cyber sleuths made the Indian community more vulnerable to cybercriminals [12]. Saxena et al. (2012) showed that necessary proactive procedures in the hands of the government and enhanced participation of the education system in the awareness of the information security approach might develop the Country's economy and lead to a strongly secured country against risks [14]. Mehta and Singh (2013) there exists a significant difference between the awareness level of employee-users and non-employee-users of internet services, and it was found that employed users have more awareness of the Indian cyber laws compared to non-employees [15]. Margit Scholl (2018) stated that Information security awareness (ISA) must be an integrated part of these agendas. As there is still essential strategic incompetence in the organizations themselves, humans should not be called "the weakest link" in the security chain. Rather, sustainable awareness-raising and training for people should be created in the organizations [16].

In a study conducted on state universities in the Southeastern United States Floyd and Yerby (2018) indicated that overall, faculty and staff had high to moderate levels of information security awareness (ISA) and behaviors. comprehensive security awareness training will be fundamental for organizations of higher education as a means of reducing threats to information technology resources [17]. Muhirwe & White (2016) conducted a study for college students at a public university in the Pacific Northwest of the United States of America and indicated that results from their study that information security awareness (ISA) significantly impacts one's information on security practice. It is therefore necessary that colleges arrange and coordinate usual information security awareness (ISA) activities that are targeted to different students and staff at different levels of study [18]. (Al-Hamar, 2019) indicated that creating a security awareness program for all employees in Qatari organizations, from senior management to the lowest job positions, will enable employees to understand the organization's security policies, in addition to their roles and responsibilities. It is vital to ensure that all employees know their tasks and roles when it comes to information security (InfoSec) since it's impossible to focus solely on technology to fix security issues that are controlled by humans. Furthermore, the organization will be responsible for any security violations if it does not establish an effective awareness program for its

employees. Moreover, the only way that the employees can employ and focus on security practices to conserve sensitive information is when they receive sufficient ongoing training in security awareness. Ongoing training would help change and improve employees' attitudes to be in line with the organization's security protection goals. And also indicated that there are many barriers and challenges to information security in Qatar, the most important is the trusting culture and the lack of awareness, which implement information security policies a challenging task. there is a clear lack of security awareness and culture amongst organizations, which makes organizations vulnerable to security breaches [19]. (Roca et al., 2019) indicated that information security (InfoSec) has become a general concern for all citizens, professionals, politicians, and decision-makers. It has also become a severe concern for societies that must protect against information security attacks, with preventive and reactive measures requiring such monitoring. It must simultaneously preserve freedom and avoid general surveillance. information security (InfoSec) is equivalent to computer security, also known as information security (InfoSec) or IT security. It protects computer systems from damage to their hardware, software, or information and disruption or misdirection of their services [20]. There is a need to establish a robust system of components to protect information integrity by strategically addressing potential threats across technical, procedural, and human aspects. This strategy is based on recognizing specific information security risks and implementing essential controls for efficient oversight and mitigation of these identified risks [21]. The state institutions are hindered in achieving full security due to underutilized network and security equipment and a lack of such equipment at some of them. Consequently, the security Infrastructure standard across these state institutions has not been effectively implemented [22].

4. METHODOLOGY

While understanding of ISA in Libyan organizations is very important, the concept of ISA is well-defined in the literature and several excellent survey instruments exist for assessing ISA. Since this study seeks to gather data from as large a sample of Libyan organizations as possible, a survey is an ideal data-gathering technique. An online survey is particularly effective over long distances and is well-suited to Libyan culture because an online survey can gather a large sample of both men and women in a short time without any ethical problems. The questions in this research were groups of semi-closed questions that combined the advantages of closed-ended questions and open-ended questions. The survey was translated into the Arabic language because the participants spoke the Arabic language. Then, the survey questions were then uploaded to Google form with all questions being optional. The survey was accessible via online links placed on the Google form. This worked well, resulting in 421 responses from adults. A survey was conducted on 421 participants who are internet users on the awareness of Information security in Libyan organizations and the age of the respondents falls between 17 to 55 years.

5. RESULTS AND DISCUSSION

5.1 Respondents' personal information

The first question was about the gender of participants. Table 2 illustrates that (62%) of the respondents are male, while (38%) of them are female.

Table 2. Respondents' Gender Representation

What gender group do you belong to? (N=421)				
	Frequency	Percent	%	Cumulative %
Male	261	62%	62%	62%
Female	160	38%	38%	100%
Total	421	100.0	100.0	

As depicted in the table.3, (35.62%) of respondents had an undergraduate degree, (24.46%) had a master's degree, (19.71%) had a diploma qualification and (8.78%) had high school. The remaining percentage was shared between Intermediate School (2.38%), and doctoral degrees (9%). This clarifies the diversity of specializations in the survey and it appears respondents were well educated considering that nearly 60% of respondents held an undergraduate degree and master's degree.

Table 3. Participant education level

What is your highest education level? (N=421)			
	Frequency	%	Valid %
Doctoral Degree	38	9%	9%
Master Degree	103	24.46%	24.46%
Undergraduate Degree	150	35.62%	35.62%
Diploma	83	19.71%	19.71%
High School	37	8.78%	8.78%
Intermediate School	10	2.38%	2.38%
Primary stage	0	0%	0%
Total	421	100	100

Table 4 illustrates the respondents' distribution across work sectors. Ministry of Communications and Informatics was the most common sector (21.62%), followed by the Education sector (21.14%), and then similar distributions of participants in the Ministry of Health and social security funds (7.12% each), (9.50%) of respondents were from the ministry of electricity, followed by the ministry of finance and banking sector (9.26%). The Ministry of Sports and Youth and the Ministry of Transportation both had the same percentage of responses (5%).

Table 4. Participant industry sector

Please select the appropriate type of sector that your organization belongs to: (N=421)				
Ministry	Frequency	%	Valid %	Cumulative %
Communications	91	21.62%	21.62%	21.62%
Education	89	21.14%	21.14%	42.76%
Electricity	40	9.50%	9.50%	52.26%
Finance and banking	39	9.26%	9.26%	61.52%
Oil and Gas	35	8.31%	8.31%	69.83%
Social Security Fund	30	7.12%	7.12%	76.95%
Health	30	7.12%	7.12%	84.07%
Economy and	25	5.94%	5.94%	90.01%
Transportation	21	5%	5%	95%
Sports and Youth	21	5%	5%	100%
Total	**421**	**100**	**100.0**	

5.2 Information security practice

The first question in this section asked if respondents physically secured (use devices locking) their portable computer devices (e.g., laptops, mobile phones). Figure 1 displays that 61.99% of respondents preserved their devices in safe places all the time because they wanted to keep their privacy. As shown in Table 5 About 24% of respondents sometimes retain their devices secure, 13.06% of respondents answered No, and 0.95% do not know whether their devices are secure or not. However, 61.99% of respondents preserved their devices in safe places all the time showing an astonishing rise of care and awareness in using these devices or the information that they contain and this is a good indicator.

Table 5. Device security

Do you keep your mobile devices (PDAs, laptop, USB keys) in a secured place and do you practice precautions to keep them secured (i.e., use locking devices) when not used? (N=421)				
Answer Options	Frequen	%	Valid %	Accumulative %
Yes, all the time	261	61.99%	61.99%	61.99%
Sometimes	101	24%	24%	85.99%
No	55	13.06%	13.06%	99.05%
I do not know	4	0.95%	0.95%	100.0%
Total		100	100	

The second question in this section asked about how secure you think information is on your computer/mobile device. 33.74% of 421 respondents said they were secure while 47.74% were not and 18.52% didn't know whenever secure or not. Hackers have a group of techniques for guessing or cracking passwords. Weak or Short passwords or passwords containing personal identification, such as name or date of birth, allow hackers to crack passwords easily. However, strong passwords composed of groups of characters including a mixture of numbers, upper- and lower-case letters, and special characters are far more difficult to crack Hackers use a set of techniques and tools such as social engineering Guess passwords, password cracking, to obtain access to users' passwords. Short or weak passwords and passwords that contain personal identification (such as name phone number or date of birth) allow passwords to be cracked easily and having a good password is still not enough to secure information; passwords should be changed regularly. However, strong passwords composed of more than 8 characters including a mixture of numbers, upper- and lower-case letters, and special characters are far more difficult to crack and so can protect information from unauthorized access or theft. Table 6 shows participants' responses to the question "Do you change your password continuously? Notably, 49.65% of respondents have never changed their passwords. It is shown that most employees are either unaware of the value of strong passwords that are changed regularly or simply don't see it as their responsibility. Even more alarming is that systems administrators in Libyan organizations do not appear to be aware of this problem either; otherwise, systems would automatically force users to select strong passwords and to change passwords regularly. 71.49% of respondents don't share their passwords with others, while 10.41% of respondents share them with their fellow and 18.1% of them share with their family members.

Table 6. Strength and Characteristics of Participants' Passwords

Do you change passwords continuously? (N=421)				
	Frequency	Percent	Valid %	Cumulative %
Daily	3	0.7%	0.7%	0.7%
Weekly	9	2.14%	2.14%	2.84%
Monthly	89	21.14%	21.14%	23.98%
Annually	111	26.37%	26.37%	86.98%
Never	209	49.65%	49.65%	100.0
Total	421	100.0	100.0	

This clarifies that employee don't share their password mostly with their family members or with colleagues, which raises the question, why share with family members or with colleagues? The high-level password sharing may be linked to the Libyan community culture in which members of the family or colleagues are seen as not trustworthy. Regardless, the security risk associated with password sharing is serious. Password strength and the frequency with which a user changes a password are irrelevant if that password is distributed to others. Table 7 shows participants' awareness of some of the main information threats and this question was multiple choices. As expected, awareness of identity theft attacks was high as was awareness of the Dos attack. However, only 95.25% of respondents are aware of viruses and malware. 68.70% of respondents know cyberstalking, 45.36% of respondents know deception and fraud, and awareness of spam emails was 23.51%. Only 33.0% of participants were aware of the Vulnerabilities probing and 33.25% of them were aware of the phishing and forgery.

Table 7. Awareness of information threats

Have you heard of and are aware of the existence of the following threats (Multiple choices)? (N = 421)			
	Responses		% of Cases
	Frequency	%	
Virus and malware	401	23.87%	95.25%
Phishing and forgery	140	8.33%	33.25%
Spam emails	230	13.69%	23.51%
Dos	99	5.89%	23.51%
Identity theft	195	11.60%	46.31%
Cyberstalking	285	16.96%	68.70%
Vulnerabilities probing	139	8.27%	33.0%
Deception and fraud	191	11.39%	45.36%
	1680	100.0%	368.89%

over 51% of respondents used antivirus software, while 43% of respondents didn't use antivirus on their devices and 6% of them didn't know if they used it or not. It is interesting to note that the use of protection software was in all cases concurrent with the awareness of related threats. For example, over 95.25% of respondents were aware of viruses and malware and 43% of respondents didn't use antivirus software, this indicates that they aren't knowledgeable of the other potential threats. Reporting security incidents is important as it allows users to find better protection solutions, and also allows security providers to reduce the likelihood of similar Information

Security incidents in the future. Unfortunately, responses show that 55.58% of 421 respondents are not aware of how or where they can report security incidents. Fig.1 shows that 44.42% of 421 respondents didn't know of creating report security incidents. This high unawareness can lower the opportunities for users to increase their security knowledge and to make a contribution to information security in Libyan organizations generally. One of the questions asked was a participant's reaction to a phone call or email asking for information. This question was included because some information threats such as fraud can be introduced by asking for personal details using email or the phone. Table 8 indicates that only 25.17% of respondents said they would answer the questions, 51.54% of the 421 respondents would never answer such a request and this is an acceptable indicator, 18.52% of respondents would ask for details before answering and 3.58% would ask colleagues for advice and 1.19% of them don't know if they respond or not.

Fig. 1 Security incident report awareness

This is a major security risk. As shown in Table.2 209(49.65%) of the respondents never change their passwords only, 111(26.37%) change their password once annually, 89(21.14%) change it every month, while 9(2.14%) change their password weekly. Conversely, 3(0.7%) of them change their password daily. In an organizational context, many organizations require staff to change their passwords regularly. However, there are some possible reasons for the high percentage of respondents who said they would not respond to emails that asked for personal information; Table 8 shows that most of the respondents willing not to provide this personal information were female. For cultural reasons, Libyan women are very

Table 8. Provision of personal information in response to an unsolicited request

How would you react if you received a phone call or an email asking for information (i.e., mobile number, personal email address)? (N = 421)				
	Frequency	Percent	Valid %	Cumulative
I never answer	217	51.54%	51.54%	51.54%
I answer the questions	106	25.17%	25.17%	76.71%
I ask for details before answering	78	18.52%	18.52%	95.23%
I ask a colleague or a friend for	15	3.58%	3.58%	98.81%
I do not know	5	1.19%	1.19%	100.0%
Total	421	100.0	100.0	

careful about their privacy when interacting with people outside their family circle. The target of the backup is to make a copy of crucial data that can be retrieved in the event of a key data failure. Initial data failures can be the result of software or hardware damage or data perversion, such as a malicious attack accidental deletion of data, or (virus or malware). Backup copies permit data to be restored from an earlier point in time to aid the business recovery from an unplanned incident. Backup the data is very important to protect against key data loss or corruption. It can use a USB or external drive stick, such as a disk storage system, or a tape drive to store data to keep it. Table 9 clearly shows that 28.74% of participants never took a backup of their data and 47.74% of the 421 respondents did a backup sometimes, but they didn't give little importance. If their data was lost by an attack, they had no method to repair it. Only 7.37 % of respondents took a copy of data every day, if the backup was ineffective, it may place them enormously at risk. There is a relationship between access to backup facilities (such as USB backup drives) and data backup, in organizations, data backup is very crucial because files may be deleted, the harm and natural disasters can happen. With an excellent backup and studied recovery plan, it is probable to recover from any of these risks.

Table 9. Data backup frequency

How often do you back up your sensitive/critical data? (N = 421)				
	Frequency	Percent	Valid %	Cumulative %
Never	121	28.74%	28.74%	28.74%
Sometimes	201	47.74%	47.74%	76.48%
Frequently	68	16.15%	16.15%	92.63%
Everyday	31	7.37%	7.37%	100.0%
Total	421	100.0	100.0	

The final question in this section asked if participants felt that privacy was important when online. Protecting online privacy is important in itself but it is also vital in avoiding identity theft. it is, with the vast majority (54.78%) of respondents either disagreeing or strongly disagreeing that online privacy is important. Unfortunately, although it is important, much of the previous data suggests that Libyans might not know how to ensure their online privacy. While much of the previous data suggests that lack of knowledge gives rise to Information Security risks. Participants were asked who was responsible for their digital privacy and were allowed to nominate more than one person or agency. Responses show that 67.6% of 421 respondents believed that they were responsible for their privacy. However, 22.8% also believed that the government was responsible, reflecting their patriarchal culture. Similarly, 35.2% of respondents believed that the company that had their digital information was responsible for its security. The tribal nature of Libyan culture may assume that other trusted parties should take responsibility, rather than individuals themselves. In comparison, in a South African study, less than 10% of respondents said that information security (InfoSec) was not their responsibility. Participants were asked Have they ever experienced a data hack or identity theft. Figure 2 indicates that 39.19% of respondents indicated that had faced these threats, 13.54% of respondents had no idea whether they had been hacked or had data stolen, and only 47.27% responded that their information not had been stolen. In reality, several of the people who indicated 'no' may not have any idea whether their information had been copied because they had no security

software to tell them. Some may have had files hacked but supposed that they had just deleted them fortuitously. Some may have files deliberately corrupted but just supposed that it was a 'bug'. It is complex to know whether information has been stolen from a computer unless the information is exposed or the user has good physical security mechanisms that can report hacking incidents.

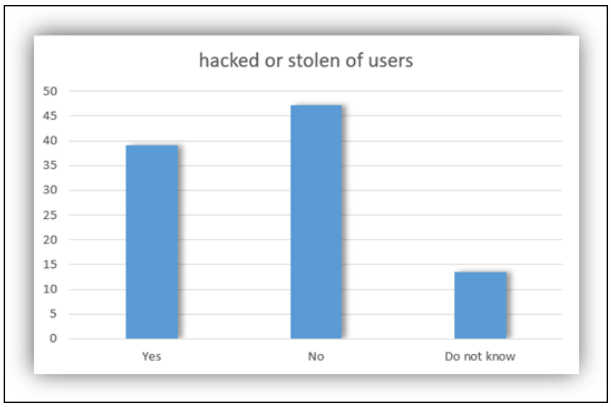

Fig. 2 Participant information stolen or hacked

This low awareness of appropriate responses would reduce the speed with which threats could be dealt with and hamper overall Information Security (InfoSec) across the country.

5.3 Preferences for information

From the data presented so far, there is a strong need to raise the level of ISA. The final two questions concerned the mechanisms by which ISA could be raised i.e.: how should information about ISA be disseminated? The Web is, by far, the most popular source of Information Security (23.7%) of 421 respondents. The Web is also particularly appropriate for Libyan culture for two main reasons. Firstly, the country is large, and much of the population lives in somewhat remote locations. The Web offers distance education which addresses this problem. Secondly, the Web is particularly suited to Libyans who could not go to attend seminars or courses. The Scientific videos from YouTube are second with 23.69%, nearly 15.22% of respondents use books, 10.34% get information from Information security experts, 9.85% use exhibitions or seminars and 6.45% choose others. Table 10 displays the list of communication mechanisms that respondents believed could effectively promote ISA. Respondents were asked to indicate their most preferred options. 19.78% of 421 respondents get information from Information security experts but over 18.14% also prefer social media pages. There is an interesting note that can be made about this Table. Firstly, the number of respondents who used the "Scientific Page on social media" option in the previous question which was about the sources that have been used to learn about information security (InfoSec) is 69.17%. This means that, apart from these options, most respondents depended on many other methods to find out about Information Security. However, when presented with a larger group of information dissemination methods (Table 10) respondents found many of them useful. For example, 23.69% nominated Scientific videos from YouTube as an effective medium but very few included Exhibitions or seminars Scientific as an "Other" mechanism that they had already used in the learning sources about the Information Security question. The greatest likely reason for this discrepancy is that respondents believed that newspapers could be very effective but that they had not previously found the information they required in newspapers. This is not surprising as Libyan newspapers are highly conservative and highly censored, so newspapers have probably paid scant attention to a problem that only affects the Web, which is a major competitor to print media. Similarly, Scientific Seminars and Exhibitions were far better and perfectly represented in Table 10 (21.62% and 26.37%, respectively) than the 1.18% "workshop" in the sources of learning about Information Security questions. Once again, the print and television media in Libya are not concerned about online information threats.

Table 10. Communication mechanisms for promoting ISA

Which communication do you think is effective in promoting awareness of information security for the public? (N=421)			
	Responses		% of Cases
	N	Percent	
Newspapers and scientific	91	5.75%	21.62%
Exhibitions	111	7.%	26.37%
Getting Information from	313	19.78%	74.35%
Scientific Page on social media	287	18.14%	69.17%
Scientific Seminars	151	9.58%	35.87%
Scientific forums and blogs on	105	6.68%	24.95%
Educational Programs and	159	10%	37.78%
Awareness Billboard/ Posters	91	5.75%	21.62%
Advertisements	97	6.13%	23.14%
Books	101	6.38%	23.99%
Cartoon series	71	4.49%	16.87%
Workshop	5	0.32%	1.18%
Total	1582	100.0%	376.71%

6. CONCLUSION

The development that takes place in internet and computer networking technology has consequently led to security challenges as evident in the increase of information threats. This development has undoubtedly necessitated new security procedures and policies to decrease the intensity of the threat and the challenges being encountered from the emergence of the new technology. The results indicate that Libyan organizations have low Information security awareness (ISA) across the departments of organizations when compared with other countries. Also, this study has indicated that information security (InfoSec) in Libyan organizations faces some serious risks from a range of threat types. It has been determined that these risks are at least partially due to low awareness of information security (InfoSec) among the public and low information security practices in organizations. There is a need to decrease the risks faced and provide good strategies for further protection from threats quickly.

7. RECOMMENDATIONS

The institutions should gather and implement a formal and well-defined business continuity and disaster recovery document and risk management that gives guidance and technical support to all members and stakeholders of the enterprise regarding the management and protection of information assets during disasters. Introduction of compulsory security awareness training for government employees. There should be a government initiative aimed at enhancing employee security awareness and knowledge, both by providing adequate training and by policing attendance if the training is made compulsory. It is also advisable that the Ministry of

Administrative Development, Labor and Social Affairs should include information security awareness (ISA) within the compulsory annual employee training courses they provide for all government employees in a bid to enhance security awareness within governmental organizations in Libya. Management of the institutions should build the information security department at the highest possible level in the institution and take the information security (InfoSec) (InfoSec) plan as an important performance measurement and should commit enough resources for the operation of information security (InfoSec) in the companies

8. ACKNOWLEDGMENTS

I would like to express my sincere gratitude to all those who contributed to the development and completion of this study. Their support, expertise, and cooperation were invaluable throughout the entire process.

8. REFERENCES

[1] Alshboul, A. (2010). Information systems security measures and countermeasures: Protecting organizational assets from malicious attacks. Communications of the IBIMA

[2] Al-Awadi, M., & Renaud, K. (2007), "Success factors in information security implementation in organizations," Paper presented at an international conference.

[3] Fadi A. Aloul, "The Need for Effective Information Security Awareness", Journal of Advances in Information Technology, Vol.3, No.3, August.2012.

[4] Alotaibi, M., & Alfehaid, W. (2018). Information security awareness: A review of methods, challenges, and solutions. Proceedings of the ICITST-WorldCIS-WCST-WCICSS-2018, Cambridge, UK, 10, 13.

[5] Ahmad, N., Arifin, A., Asma'Mokhtar, U., Hood, Z., Tiun, S., & Jambari, D. I. (2019). Parental awareness on cyber threats using social media. Jurnal Komunikasi: Malaysian Journal of Communication, 35(2), 485-498.

[6] Kaspersky Lab (2022) http://www.securelist.com/en/analysis/204792101/Kaspersky_Security_Bulletin_2009_Statistics _2009, accessed 29/02/2010.

[7] Cox, J. 2012. Information systems user security: A structured model of the knowing-doing gap. Computers in Human Behavior, 28:1849-1858.

[8] Alotaibi, F.; Furnell, S.; Stengel, I.; Papadaki, M. A survey of cyber-security awareness in Saudi Arabia. In Proceedings of the 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), Barcelona, Spain, 5–7 December 2016.

[9] Alotaibi, M., & Alfehaid, W. (2018). Information security awareness: A review of methods, challenges, and solutions. Proceedings of the ICITST-WorldCIS-WCST-WCICSS-2018, Cambridge, UK, 10, 13.

[10] Bhushan K. (2012), India ranks fifth among cybercrime-affected countries, retrieved from http://www.thinkdigit.com/Internet/India-ranks-fifth-among-cyber-crimeaffected_9476.html on September 5, 2012.

[11] Jamil D. and Khan M.N.A. (2011), Data Protection Act in India with Compared to the European Union Countries, International Journal of Electrical & Computer Sciences, Vol: 11 No: 06.

[12] Pandey K. (2012), Low security makes netizens vulnerable to cybercrimes, retrieved from http://articles.timesofindia.indiatimes.com/indore/31863717_1_cyber-crimes-cyber-cellcyber-criminals on May 26, 2012

[13] Dalal P. (2010), Awareness of Cyber Law in India, retrieved from http://cyberlawsinindia.blogspot.in/2010/05/awareness-of-cyber-law-in-india.html on September 03, 2012

[14] Saxena P. et al. (2012), A Cyber Era Approach for Building Awareness in Cyber Security for Educational System in India, IACSIT International Journal of Information and Education Technology, Vol. 2, No. 2.

[15] Mehta, S., & Singh, V. (2013). A study of awareness about Cyber Laws in the Indian Society. International Journal of Computing and Business Research, 4(1), 1-8.

[16] Scholl, M. C., Fuhrmann, F., & Scholl, L. R. (2018). Scientific knowledge of the human side of information security as a basis for sustainable training in organizational practices.

[17] Yerby, J., & Floyd, K. (2018, August). Faculty and staff information security awareness and behaviors. In Journal of The Colloquium for Information Systems Security Education (Vol. 6, No. 1, pp. 23-23).

[18] Muhirwe & White (2016) conducted a study for college students at a public university in the Pacific Northwest of the United States of America and indicated the results from their study.

[19] Al-Hamar, Y., Kolivand, H., & Al-Hamar, A. (2019, October). Phishing attacks in Qatar: A literature review of the problems and solutions. In 2019 12th International Conference on Developments in eSystems Engineering (DeSE) (pp. 837-842). IEEE.

[20] Roca, S. K.-L.-D.-V. (2019). Cybersecurity Current Challenges and Inria's Research Directions. Le Chesnay Cedex, France: Inria.Bowman, M., Debray, S. K., and Peterson, L. L. 1993. Reasoning about naming systems.

[21] Salima. B ,Almabruk ,S , Awad.E , 2020 . Assessment of Security Issues in Banking Sector of Libya, International Journal of Computer Applications, Vol 176 (13), 975 – 8887.

[22] Almabruk, S., & Khaled, E., (2023), The Digital Infrastructure Standard for Assessing the Quality of Higher Education Institutions: A Case Study of Libyan State Universities. In Proceedings of The Second International Conference 2023 on Quality of Education and Digital Transformation: Reality and Future Bets, Special Issue, Benghazi, Libya, 1-9.