Building an Information Security Awareness Program for a Private Financial Organization: Case from Libya

Salima Benqdara
University of Benghazi
Benghazi, Libya

ABSTRACT
The protection of assets of organizations became one of the major aspects that organizations have to deal with. The issue is too serious when it comes to financial organizations due to their sensitivity to data security attacks. Security breach incidents can happen in an organization no matter how well the technology is protected. The main reason for this is employees' improper conduct or lack of action that leads to the majority of information security incidents. Educating employees to improve information security awareness plays a significant part in securing organizational environments. Although, best practice, standards provide a set of minimum information security awareness controls that should implement. This study proposes an information security awareness training program to improve knowledge of information security and improves employee behavior for a private financial organization in Libya.

General Terms
Security awareness-training program.

Keywords
Information security, Information security awareness program, Information security policy.

1. INTRODUCTION
Information is an organization's most important asset, and protecting this asset is becoming one of the major issues organizations must deal with. The need for secured and protected information system assets in any organization has become a very important component. Most organizations focus only on technology solutions and often pay too little attention to the most important and weakest component of security, which is the human factor[1]. In a 2018 Computer Security Breaches Survey conducted jointly by the UK Department for Digital Culture and The University of Portsmouth, it was established that fraudulent emails or being directed to fraudulent websites account for the most common security risk which stands at about 75% and 74% for businesses and charities respectively. Others impersonating organizations in emails or online is now the second most common security risk, which stands at 28% and 27%. Viruses, malware, and spyware attacks come in at third at 24%, which is more common than denial of service attacks at 12% and 13% while hacking and attempted hacking happen at 3% and 2% [2]. Today's security problems are primarily due to inadequate security awareness by users, which can mitigate without the need for security technologies. It confirms that individual staff members commonly spot the most disruptive breaches. The human factor in security is more critical than technology [3]. Organizations in the public and private sectors need to enhance employees' information security awareness and knowledge by providing security awareness and education programs.

Information security awareness is used to refer to a state in which users in an organization are aware of and ideally committed to their security mission, and is often expressed in end-user security guides [4]. Information security awareness is a serious matter when it comes to information security practices or procedures. They can also be misused, misinterpreted, or misused by end users and lose their actual usefulness. Although security awareness-related matters range from simple information security guidelines to well-developed information, security education programs [5]. Security awareness and training are important components of any information security program. Fundamentally, training and awareness programs serve to facilitate and improve security compliance processes and the overall security of an organization. The primary goal of security education and awareness is to change user behavior and increase overall security awareness. Security awareness efforts are designed to change behavior or reinforce security best practices [6].

Security awareness delivers knowledge about information security (including how to identify various attacks, how to reduce one's risks of becoming a victim of cyber attackers, and who shall contact in case of questions and incidents). These programs may include security awareness and education measures that cover different aspects and topics. Cybersecurity training programs can take many forms, to communicate the best cybersecurity practices, inspire employees to change their cyber-insecure behaviors and improve cybersecurity behavior over the long term [7]. Cybersecurity training is progress designed to help employees understand their role in addressing information security exposures. This awareness training will help employees to understand risks and identify potential attacks such as when they receive email or use the web. An employee who perceives high vulnerability to his organization's information systems will be more willing to take protective actions. There are significant challenges, therefore, in ensuring that people are both aware of cybersecurity risks and can respond to those risks in a meaningful way. Simple policy campaigns or warning messages, intended to increase their awareness of the risks involved are not always effective, as they implicitly rely on users making very informed or rational decisions [8].

This study proposes an information security awareness training program to improve knowledge of information security and improves employee behavior for a private financial organization in Libya. The rest of the paper is organized as follows: Section 2 discusses the related works. Section 3 presents the proposed approach. The results and discussion of findings are presented in Section 4. Section 5 concludes the paper.

2. RELATED WORK
Bada and Nurse (2019) propose a cybersecurity education and awareness program for small- and medium-sized companies in Australia, the UK, and the USA. This program consists of five

steps (i) initial engagement with SMEs's (ii) improving security practices and culture (iii) program resources (iv)Trusted third-party resources/services and (v) communication strategy. The study found that awareness is an important element to change behavior. On the other hand, it cannot be enough to change behavior only many cultural factors affect human behavior.

Amar and Shailendra (2023) examine customer awareness and satisfaction with cybersecurity in the digital transformation of banking in Saudi Arabia. Data was collected from 355 banking customers in Saudi Arabia. Three important phases of cybersecurity, including cyberattacks, phishing, and hacking, are analyzed through several dimensions. To study the impact of a cyberattack, phishing, hacking, cybersecurity assistance, and desires on cybersecurity's technical awareness on customer satisfaction ANOVA and bivariate regression analysis are used. The results show that customers need more satisfaction on security level aspects from the bank's side, and banks should provide awareness and training programs to protect customers from cyberattacks.

Rowe et al. (2012) proposed a study to define the impact of cybersecurity education tools in nine businesses in different businesses with 1 to 160 employees. Improved recommendations for policies and training were developed and implemented for a year with pre- and post-interviews used to assess the effect on knowledge and behavior and employment. The authors decided that a small amount of basic cyber security training for employees improves a company's security position. The author's findings are that the cost of existing training may be too high for small- and medium-sized businesses. The authors also recommended additional research on providing free, quality resources for small businesses and possible government incentives for small- and medium-sized businesses to invest in cybersecurity products, services, and training.

Stefan et al., (2017) proposed a study to analyze IS managers' efforts to design effective ISA programs by comparing current design recommendations suggested by scientific literature with actual design practices of ISA programs in three banks. Moreover, this study addresses how users perceive ISA programs and related implications for compliant IS behavior. In this study, a multiple case design to investigate three banks from Central and Eastern Europe. The paper contributes to IS compliance research by offering a comparative and holistic view of ISA program design practices. The study found that influences on users' perceptions centered on IS risks, responsibilities, ISP importance and knowledge, and neutralization behaviors. Finally, the study raises propositions regarding the relationship between ISA program designs and factors, which are likely to influence users' ISP compliance.

Lemma et al., (2019) proposed an information security awareness program for Enat bank in Ethiopia. The research attempted to answer three questions (what is the current information security awareness creation practice at Enat Bank? what should the topics of an information security awareness program for Enat Bank be? and how should the information security awareness program be organized to deliver the necessary information to Enat Bank employees?). The result showed that the level of information security awareness of Enat Bank employees is unsatisfactory. Based on the results, the research introduces a program that will assist the bank in terms of creating information security awareness and good practices for its employees to reinforce its security posture by mitigating vulnerabilities for computer attacks. Moreover, a strategy was proposed to help the bank smoothly implement the program. In addition, Recommendations are forwarded on a short and long-term basis to improve the information security awareness of its employees.

Reinheimer et al., (2020) present a field investigation in a German organization from the public administration sector to evaluate the effectiveness of their security awareness and education program in phishing. The study find a significantly improved performance of correctly identifying phishing and legitimate emails directly after and four months after the program's deployment.

Salima et al. (2020) proposed a framework to assess the information security issue in Libyan banks. The study aimed at the assessment of security strategy in Libyan banks to identify security gaps. To achieve the aim of this study data was collected by interviewing information security staff to evaluate the current security strategy in Libyan banks. In this study, data was collected on the current security situation for some of the banks in Libya and then analyzed using the risk assessment matrix and static tool to identify the critical assets that need to be protected. During data analysis, vulnerabilities were mapped to known potential threats and the impact of these threats on security characteristics. CIA was determined Based on the probability and impact of the bank's information, availability and confidentiality were the most affected by the current security flaw. The results showed that there is no deployment to the standard, in reality; Information security management is free to choose the appropriate standards for the bank. The results showed that there are security gaps in the current security system that is responsible for sharing customers' information as to their requests. The study concluded that the management of information security in Libyan banks should improve its processes and be aware of the benefits and advantages arising from information security standards. Furthermore, Libyan banks should implement a comprehensive and adequate set of information security components that aid in addressing threats on the technical, process, and people levels based on identified information security risks and the appropriate controls that are necessary to mitigate the identified risks.

3. PROPOSED APPROACH

This study proposes an information security awareness training program to improve knowledge of information security and improves employee behavior for the private financial organization in Libya.

3.1 DATA COLLECTION AND ANALYSIS

The organizations selected for this study are Case A - a private organization for financial services, and Case B, which represents participants from private banks in Libya. The population of the study is limited to managers and IT staff in some of the private financial organizations in Libya. Analyzed both companies by creating a scope for the number of employees and department involved in the program, and categorized the program according to the critical position each department have in the company. In this study, data was collected to assess the Information Security Awareness (ISA) in privet financial organizations. The results showed that there are security gaps in the current Information Security Awareness (ISA), which is responsible for a lack of users' ISA. The overall information security awareness of privet financial organizations is not favorable for the protection of information assets. There is no appropriate foundation for defining how information security should manage in privet financial companies. Analysis of results identified the key strengths of weaknesses and that areas need improvement. Which helped in

constructing the topics for the information security awareness training program.

3.2 PROPOSED TOPICS

This study proposed an approach to providing an information security awareness training program to improve the security standard in private financial services and banks in Libya. According to research conducted previously, awareness programs should not be constructed randomly without depth analysis that focuses on candidate behavior and security background. This helps the topic be effective and provides key points that can improve the security approach when the incident occurs. In addition, the topics need to be up to date according to technological advances. The key findings of the analysis are associated with the candidate topics that must be included in the information security awareness training program to improve the security standard in private financial services and banks in Libya. The key findings of the analysis are associated with the candidate topics in Table 1.

Table 1: key findings of the analysis are associated with the candidate topics

Key Finding	Candidate topic
Vulnerable to malware breach	malware techniques and tactics
Lack of understanding of the CIA	Introduction of CIA
lack of importance of data	Data classification
The employee does not understand the risk of phishing and is not able to distinguish if the email is legitimate or not	• Introduction to phishing and type of phishing • Tactics and techniques of phishing • Cycle o phishing attack • The key point to identifying the phishing email
Vulnerable to the ransomware attack	• Introduction to ransomware • Type of ransomware • Cycle of ransomware
Unable to identify the site that is safe to browse	• Consequences of reckless browsing • Steps to browse safely.
Lack of policy	Introduction to policy and its importance
Weak Password	Strong Password characteristic
Usage of removable media	Risk of using removable media
Not familiar of risk working remotely	• Working remotely with safe techniques • Consequences of working remotely
not familiar with the risk that mobiles on the organization and personal	• Tips for securing mobiles in the organization • Consequences of mobiles on the organization and personal
Risk of Spyware	• Introduction to spyware • Spyware tactics.

3.3 DELIVERY TECHNIQUES

In this study, Company A never has conducted an awareness program before on the other hand company B conducted several online awareness programs. However, the data on employee behavior and the culture barrier shows that online awareness training programs are ineffective because computer security is a very sophisticated topic and employees require absolute attention to understand the risk of it. In addition, employees require real-life examples and live practical examples in computer security, so the subconscious of the candidate relates the security scenarios to his own experience. In addition, discussion and questions are crucial for the candidate to understand the importance of security for the organization's benefit. Thus according to the analysis conducted for the above show company A and B recommended using lecture and practical methods. The below techniques have been used in the information security awareness training program.

- Face-to-face lecture and practical explanation
- Live tutorial
- Security Educational Videos
- Graphs and pie charts of security data breach loss
- Questions and discussion
- Real-life examples and possible solutions
- Security case study

3.4 Evaluation

Evolution is the last stage of the program that focuses on identifying the improvement of employees after conducting the awareness program. However, the discussion of the result will be clarified in the result section, which will focus on explaining the improvement of the employee in each category.

4. RESULTS AND DISCUSSION

4.1 Company A

Table 2 summarizes the result of the information security awareness-training program of Social engineering, Policy, Security Knowledge, awareness, and Physical security for the IT department in company A. The result shows an improvement of 73.4% for the IT department in company A for social engineering. This indicates that the strongest asset in security in the organization was the huge vulnerability itself of the organization. Although, the result shows an improvement with 66.6% and 67.5% for the IT department In terms of policy

and Security Knowledge respectively. Moreover, The result shows an awareness improvement of 80%, and the Physical security achieved 40% for the IT department. The result shows the greatest increase in the level of employee awareness appears to be observed after training at Company A.

Table 2: Improvement percentage indication in information security awareness training program for IT

Category	Company	Improvement percentage
		IT
Social engineering	Company A	73.4%
Policy	Company A	66.6%
Security Knowledge	Company A	67.5%
Awareness	Company A	80%
Physical security	Company A	40%

Table 3 summarizes the result of the information security awareness-training program of Social engineering, Policy, Security Knowledge, awareness, and Physical security for the managers in company A. The result shows an improvement of 75.5% for managers in company A for social engineering. Although, the result shows an improvement of 50% and 55% for managers In terms of policy and Security Knowledge respectively. The result shows an awareness improvement of 77.5% and Physical security achieved by 40% for managers. Managers in company A showed exceptional focus and determination to improve since the first day in the program. The result shows the greatest increase in the level of employee awareness appears to be observed after training at Company A.

Table 3: Improvement percentage indication in information security awareness training program for managers

Category	Company	Improvement percentage
		Managers
Social engineering	Company A	66.33%
Policy	Company A	50%
Security Knowledge	Company A	55%
Awareness	Company A	77.5%
Physical security	Company A	40%

Figure.1 outlines the information security awareness-training program of Social engineering, Policy, Security Knowledge, awareness, and Physical security for the IT department and managers in company A. The result carried out improvement after training with 73.4% and 75.5% in social engineering for the IT department and managers. Although In terms of policy, the result shows an improvement with 66.6% and 50% for the IT department and manager .in addition, significant improvement in knowledge of information security was achieved by 67.5% and 55% after training for the IT department and managers. Awareness achieved the highest improvement with 80% and 77.5% for IT and managers, respectively, and Physical security achieved 40% for IT and 40%f managers. The figure below shows that the IT department achieves the highest improved knowledge of information security compared with managers. IT department employees' became more capable to distinguish if the email they have received is legitimate or a phishing email. In addition, they are well aware of the right approach that needs to be taken when the incident occurs. Moreover, understood the risk and consequences that a lack of policy produces. They become capable to build their policies in creating a secure environment to secure their critical assets. Furthermore, the IT department became well aware of the consequences that cyber-attacks can initiate on the organization for either the long term or short term. According to the results, employees understood the risk of cyber-attack which led to improving the security standard in the company; also, employees become aware of the irresponsible behavior they used to perform daily. Employees understood the importance of awareness for both groups and the results would improve if company A consistently provided at least twice a year. Which will increase the security importance to the organization's ecosystem. in terms of physical security, the company improved slightly compared to the rest of the categories because physical security is already implemented, and the company is aware of it. The result shows the greatest increase in the level of employee awareness appears to be observed after training at Company A and the understanding of the risk they might cause due to lack of security awareness. The security improvement overall indicates that the IT department lacked guidance in security. Thus, a security awareness-training program not only increases employee knowledge of information security but also had a significant impact on actual employee behavior in this sphere.

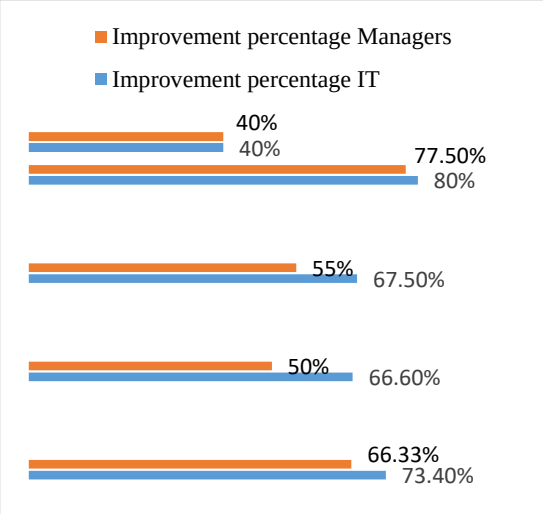

Fig. 1. Improvement percentage indication in information security awareness training program

4.2 Company B

Table 4 presented the result of the information security awareness-training program of Social engineering, Policy, Security Knowledge, awareness, and Physical security for the IT department in company B. The result shows an improvement of 75.5% and 67.6% in terms of social engineering and policy for the IT department, respectively. Furthermore, the result shows an improvement of 67.6% for the IT department in Security Knowledge. The awareness improvement with 82.2% and Physical security achieved 35% for IT, respectively. The results find that there is the greatest improvement was observed in employees' awareness after training in Company B.

Table 4: Improvement percentage indication in information security awareness training program for IT

Category	Company	Improvement percentage
		IT
Social engineering	Company B	75.5%
Policy	Company B	67.6%
Security Knowledge	Company B	71.4%
Awareness	Company B	82.2%
Physical security	Company B	35%

Table 5 presented the result of the information security awareness-training program of Social engineering, Policy, Security Knowledge, awareness, and Physical security for the managers in company B. The result shows an improvement of 64.7%% and 45% in terms of social engineering and policy for the managers, respectively. Furthermore, the result shows an improvement of 45% for the managers in Security Knowledge. The awareness improvement with 73.5% and Physical security achieved 35% for managers. The results find that there is the greatest improvement was observed in employees' awareness after training in company B.

Table 3: Improvement percentage indication in information security awareness training program for managers

Category	Company	Improvement percentage
		Managers
Social engineering	Company B	64.7%
Policy	Company B	45%
Security Knowledge	Company B	45%
Awareness	Company B	73.5%
Physical security	Company B	35%

Figure.2 illustrates the information security awareness-training program of Social engineering, Policy, Security Knowledge, awareness, and Physical security for the IT department and managers in company B. The result carried out improvement after training with 75.5% and 64.7% in social engineering for the IT department and managers. Although In terms of policy, the result shows an improvement with 67.6% and 45% for the IT department and manager .in addition, significant improvement in knowledge of information security was given by 82.2% and 73.5% after training for the IT department and managers. Awareness achieved the highest improvement with 82.2% and 73.5% for IT and managers, respectively, and Physical security achieved 35% and 35% for IT and managers, respectively. According to the results, management employees understood the tactics and techniques that social engineers

perform to manipulate their target and become more confident and capable to take the right action when they receive emails from illegitimacy sources. IT department understood in depth how they could mitigate the risk and they improved in distinguishing the severity of risk when ransomware hit the company. The rock improvement made by the IT department shows they are capable to create policies that will help the company perform decently when an incident occurs. Which is considered an asset for the organization. However, the results from management employees show the acknowledgment of the benefit of implementing strong passwords that will be very hard to crack by threat vectors, which will help secure the client data. In addition, the improvement indicates the acceptance of future policy when a company implements it. Furthermore, the IT department became well aware of the consequences that cyber-attacks can initiate on the organization either for the long term or for the short term. IT department improved significantly in understanding the risk of having vulnerability such as LOG4J level in the network and the right procedures to mitigate the threat such risk can initiate which will improve the security standard in the organization. Employees understood the importance of awareness for both groups and the results would improve if company B consistently provided at least twice a year. Which will increase the security importance to the organization's ecosystem. Both companies improved slightly compared to the rest of the categories because the physical security is already implemented, and the company is aware of it. The security awareness-training program helps employees learn about information security, and it has a big impact on how they behave in this area.

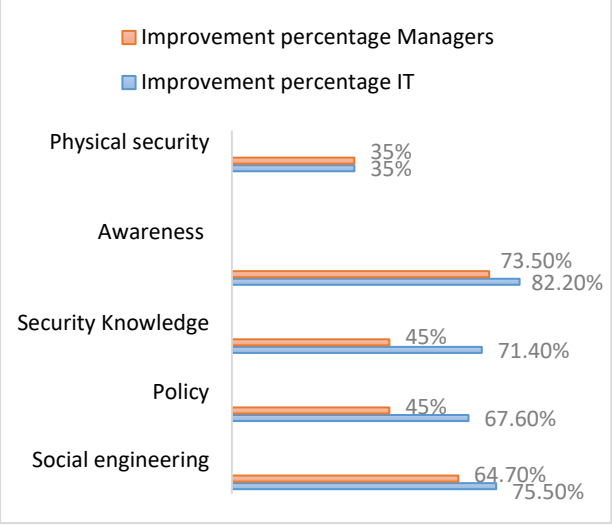

Fig. 2. Improvement percentage indication in information security awareness training program

5. CONCLUSION

Information security incidents in an organization are not only determined by technology but also by people. Employees' improper conduct or lack of action leads to the majority of information security incidents. Therefore, employees' understanding of the consequences of their behavior is key to the security of the organization's information security systems. The Awareness Training program is an effective method of affecting employee awareness in the area of information security. The results show a significant improvement in most of the security categories in Company A and B; also, the companies have the quality to construct a well-secure environment. Concurring to the results, management employees understood the tactics and techniques that social engineers perform to manipulate their target and become more confident and capable to take the right action when they receive emails from illegitimacy sources. IT department understood in depth how they could mitigate the risk and they improved in distinguishing the severity of risk when ransomware hit the company. The rock improvement made by the IT department shows they are capable to create policies that will help the company perform decently when an incident occurs which is considered an asset for the organization. Moreover, the results from management employees show the acknowledgment of the benefit of implementing strong passwords that will be very hard to crack by threat vectors, which will help secure the client data. In addition, the improvement indicates the acceptance of future policy when a company implements it. Furthermore, the IT department became well aware of the consequences that cyber-attacks can initiate on the organization either for the long term or for the short term. Employees understood the importance of awareness and the results would improve if companies consistently provided at least twice a year which will increase the security importance to the organization's ecosystem. The security awareness-training program helps employees learn about information security, and it has a big impact on how they behave in this area. The results concluded that the great effectiveness of the information security awareness-training program as a method of not only improving knowledge of information security but also mainly one that has a significant impact on the actual IS behavior of employees. Thus, the security issue was that the board of the company has not contributed intensely to make a secure environment to ensure their client information from risk.

6. REFERENCES

[1] Tse, W., Hui, M., Lam, S., Mok, Y., Oei, W., Tang, K., and Yau, X. 2013. Education in IT Security: A Case Study in Banking Industry, GSTF Journal on Computing (JoC). 3(3), 21-30.

[2] UK Department for Digital, Culture, Media, and Sport .2018. Cyber Security Breaches Survey 2018: Statistical Release". Retrieved 6th Aug 2020 from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf

[3] Alotaibi, F.G., Clarke, N. and Furnell, S. 2020. A novel approach for improving information security management and awareness for home environments. Journal of information and computer security. 29 (1), 25-48.

[4] Siponen, M., Pahnila, S., and Mahmood, M. 2010. Compliance with Information Security Policies: An Empirical Investigation. Computer, 43(2), 64-71.

[5] Siponen, M. 2000. A conceptual Foundation for Organizational Information Security Awareness. Information Management & Computer Security. 8(1), 31-41.

[6] Amare, B.2015. Assessment of Insider Threat in Ethiopian Banking Industry. Thesis work, Addis Ababa University, Addis Ababa.

[7] Katz, I. 2017. "Cybersecurity awareness training: How to improve employee security behavior,"

[8] ACQUISTI, G. L. , ALESSANDRO, B.and LAURA. 2015. "Privacy and human behavior in the age," Science (80-). vol., 347(6221), 509–514.

[9] Bada, M., and Nurse, J. R. 2019. Developing

cybersecurity education and awareness programming for small-and medium-sized enterprises (SMEs). Information & Computer Security.

[10] Amar,J., Shailendra K. 2023. "Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital Transformation". Human Behavior and Emerging Technologies. vol., 2023. https://doi.org/10.1155/2023/2103442

[11] Rowe, B., Ladd, K., Scheper, C., Kaydos-Daniels, S., Piskin, K. and Myers, J.2012. Cyber security test bed: Summary and evaluation results.

[12] Stefan Bauer and Edward W.N. Bernroider and Katharina Chudzikowski. 2017. Prevention is better than cure! (). Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. Computers & Security, Vol 68, 145-159.

[13] Lemma, L ., Solomon, N., Milkyas, B. 2019. Building an Information Security Awareness Program for a Bank: Case from Ethiopia. In proceeding of July 2019 Conference: Twenty-fifth Americas Conference on Information Systems At Cancun, Mexico.

[14] Reinheimer, B., Aldag, L., Mayer, ., Mossano, M., Duezguen, R. , Lofthouse, B., Von Landesberger, T., Volkamer, M. 2020. .An Investigation of Phishing Awareness and Education over Time: When and How to Best Remind Users, SOUPS'20: In Proceedings of the Sixteenth USENIX Conference on Usable Privacy and Security August, 259–284.

[15] 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.