The Need for Effective Information Security Awareness in Private Financial Company: Case from Libya

Salima Benqdara
University of Benghazi
Benghazi, Libya

ABSTRACT
The increase in cyber-attacks causes individuals and businesses to face financial loss and reputation damage. Most studies in information security ignore human factors and focus only on information security technological countermeasures, while the security culture of employees is vital for financial organizations. Financial organizations need to ensure that the interaction between employees and the information security system, contributes to the protection of information assets. The purpose of this study is to assess the security gap between how far technology has advanced and how much employees are aware of it. The study indicated that there is a serious problem with information security awareness in private financial organizations. The study concluded that the overall information security awareness of private financial organizations is not favorable to the protection of information assets. There is no appropriate foundation for defining how information security should manage in private financial organizations and the risk identification process. The study recommended that private financial organizations should implement information security awareness and training programs and implement a formal information security policy that aids in addressing threats on the technical, process, and people levels.

General Terms
Security awareness

Keywords
Information security, Information security awareness, Information systems, Information security management.

1. INTRODUCTION
Information security has always been a major concern for organizations over the past years. The advance in technology enables employees to work from various devices and reach information from anywhere at any time. This new situation increases user productivity and the efficiency of business processes. However, the weakest links in any organization's security defenses are its employees[1]. Security can never be achieved by just trying to prevent attacks on a technical level and not bothering the employees. To reduce the incidence and severity of employee attacks, it is necessary to raise the level of information security awareness of ISA within the organization. Information Security policies and procedures are commonplace 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 [2].

Information security policy is the role and responsibility of employees to protect the information system and technological resources of their organizations [3]. These policies are implemented to help employees to manage technological resources and managers of organizations should help the employee to follow these policies [4]. Regularly, organizations adopt/create IS security policies for the sake of compliance with international standards or governments, hence these policies fail to provide reliable security as they only remain in documents and are not practicing [5]. Management fails to enforce policies to users and provide them with appropriate knowledge and regular training to equip them with reliable tools and knowledge about organization IS security.

Today, cyber-attacks that are part of national security, are becoming a threat to both developed and emerging countries. It is difficult to detect the cyber threat and hard to predict its long-term effects. However, cyber security awareness is growing among executives and most organizations are still inactive. Proactive would bring success to organizations in managing cyber risks. It would be useful to personalize the risks for managers so that they can realize the vulnerability and the effects [6].

Security awareness efforts are designed to change behavior or reinforce good security practices. The purpose of awareness performances is basically to focus attention on security. Awareness presentations are proposed to allow individuals to recognize IT security concerns and respond accordingly. In a research conducted with 579 business professionals in the USA, the results show that the employees who are aware of their companies' information security policies and procedures behave more securely compared to the ones who are unaware. In the same research, it is also found that an organizational information security framework affects the employees' threat evaluation and coping skills positively which makes a meaningful contribution to cyber security behaviors. Through preparing cyber security awareness programs and measuring the results, the organization may foster awareness and close the gap between secure employees' behaviors and risk perception. Procedures are needed to motivate employees to learn security policies and act securely [7].

This paper has proposed a framework to assess Information Security Awareness (ISA) in privet financial organizations in Libya. The objective of this study is to assess the security gap between how far technology has advanced and how much employees are aware of it. 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. Finally, Section 6 recommendations

2. RELATED WORK
Due to the importance of clustering many researchers have devoted time to design new algorithms as well as to improve the existing algorithm's performance and clustering quality with new meta-heuristic approaches.

He et al., (2019) proposed a study to investigate the effect of different evidence-based cybersecurity training methods on employees' cybersecurity risk awareness and self-reported behavior. The study participants were allocated into four groups to assess the effects of cybersecurity training on their

perceptions of vulnerability, severity, self-efficacy, security intention, and self-reported cybersecurity behaviors. The results show that an evidence-based malware report is a relatively better training method in affecting employees' intentions of engaging in recommended cybersecurity behaviors compared with the other training methods used in this study. A closer analysis suggests whether the training method contains self-relevant information that could make a difference to the training effects. The Author recommends regular cyber security awareness training for all employees to prevent data breaches of intellectual capital. Cybersecurity awareness seems to be the starting point of this hard task, to fight cyber-attacks, although it is very challenging in organizations.

Accenture (2019) presents interviews with more than 2,600 security and information technology (IT) professionals at 355 organizations worldwide. The Author found that the companies' losses due to malware increased 11 percent, to more than US$ 2.6 million per company. whereas, the cost due to malicious insiders such as employees, temporary staff, contractors, and business partners, jumped by 15 percent, to US$ 1.6 million per organization, on average. Together with advanced protections regarding hardware and software, the companies must not ignore a vital dimension of security, which is the "human factor".

Adam et al., (2019) propose a study to examine factors affecting the information security system for computer users, which contain organizations and individuals. The study found that the solution of applying social technical theory by providing employees with appropriate training will help in changing their beliefs and norms that can change their perception of organization security. Suitable and fixed training can help in changing employees' trust and sense of privacy about information security. Awareness about information security policies will help protect these policies are being esteemed and followed. Understanding how various work environment situations can affect information system security will help both managers and employees in securing information security. Therefore, understanding all these factors and providing training and awareness programs to both managers and users will help strengthen the organization's information security.

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 which 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.

salima (2019) presented a study to assess the security status of Wireless Local Area Networks (WLAN) used by occupants and coffee houses in two noteworthy city communities in Libya. The objective is to assess the security vulnerabilities that lie underneath the use of WLAN by the general population in Libya. Information gathered from different populated locales and analyzed to better understand the wireless security awareness among the public. security issues of wireless local area networks in Elbrega and Ajdabiya were surveyed and analyzed. The results indicate that the security standard is low due to a lack of awareness in the IT community in that particular city. The survey shows that the wireless network that is using WEP is more vulnerable than the work that uses the recent configuration (WPA2) since the WPE 24-bit initialization vector and weak authentication. To secure the wireless network need change the default SSID Implement a sophisticated password and configure the encryption to WPA2.

Al-Shanfari et al., (2022) recommended a comprehensive theoretical model based on the Protection Motivation Theory for assessing employees' intentions for information security behavior. The study used a survey and the structural equation modeling (SEM) method. The study found that risks and behaviors should impact the awareness efforts and Employees must be provided with Information Security Awareness (ISA) programs and evaluated constantly. Furthermore, the research model has been extended to include facilitating conditions that help make sure that actual InfoSec behavior is in line with information security regulations and policies.

Emad Shafie (2022) proposed a study to address cybersecurity issues in the private sector. The survey data was gathered from IT managers of private organizations and analyzed for descriptive statistics. The study shows that Saudi private organizations do not contribute sufficiently to cyber security. The tendency for security management needs to review because of its risks. IT managers do not have adequate knowledge or skills to anticipate the possibility of cyber-attacks and risk assessment procedures for practical and mitigation strategies. They do not even have the skills to detect internal security threats.

Mukesh et al., (2016) introduce the concept of social engineering, different types, common ways of attack, and related case studies. The study discussed several ways to protect against social engineering through proper education, training, procedures, and policies. Finally, the study highlights the fact that social engineering has developed to be one of the effective threats to information security, and should increase the importance of its innovative complements.

3. PROPOSED APPROACH

This paper has suggested that the level of attacks may be due to a lack of Information Security Awareness (ISA) among the Libyan public. The organizations selected for the study are Case A - a private organization for financial service, and Case B which represent 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.

The face-to-face interview stage initiated with security discussion in different security categories that will identify candidate skills in security, which will help the analysis, be made from a security and behavioral perspective, which will give a clear understanding of the culture of the organization. The Interviews are conducted with managers and IT staff to collect the data in each of the case study organizations. The study aimed at the assessment of the security strategy to identify security gaps in a private financial organization in Libya. In our case, we prefer to use interview questions for much more accurate results because previous research questionnaires provided inaccurate results compared to a face-to-face interview.

Analyzed the data collected to assess the level of Information Security Awareness (ISA), and current practices related to information security and identify security gaps in the private financial organization in Libya. After analyzing the behavior and the data of each category the result shows the strength and weaknesses and if the strength is, obtain from employee hard work (self-taught) or training provided by the company. This will help the analyzer to identify the cause of the lack in the category from the recklessness of employees or lack of security support from the company. In addition, the analyzer will be able to list the areas, which require improvement. The questions of the interview are prepared in advance; they are mapped to seven categories of data as shown in Table 1 to assess their awareness and review their current practices related to information security:

Table 1: Mapping interview questions to interview aspects

Category	N of question	Highlight
Social engineer	5	• Phishing • Phishing life cycle • Phishing methods • Ransomware
Policy	5	• Segregation of duties • Password policy • strong Password characteristics • organization policy
Security knowledge	5	• CIA • Vulnerability risk and threat • Security best practices
Awareness	5	Is the employee aware of the following: • Incident report procedures • Company policy • Password policy • Clear disk policy
Physical Security	5	Availability of the following • CCTV • Log access to the Datacenter • Safety procedure for the data center
		• Disposing of sensitive data

4. RESULTS AND DISCUSSION

4.1 Company A

Table 2 summarizes the result of the Information Security Awareness (ISA) assessment of Social engineering, Policy, and Security Knowledge for the IT department in company A. The result shows that 30.52 % and 39.14% only know social engineering and policy. In terms of Security Knowledge, the results showed that 45.40% know information security. It appears that there is a lack of awareness of Social engineering, Policy, and Security Knowledge in the IT department in company A. unfortunately these results indicate that company A security standard is below average, due to a lack of experience security engineers and a lack of security department responsible to construct security defense. These results indicate that Company A is vulnerable to reconnaissance attacks.

Table 2: Social engineering, Policy, and Security Knowledge assessment for IT staff

Category	Highlight	Percent
Social engineering	• Phishing • Phishing life cycle • Phishing methods • Ransomware	30.52%
Policy	• Segregation of duties • Password policy • strong Password characteristics • organization policy	39.14%
Security Knowledge	• CIA • Vulnerability risk and threat • Security best practices	45.40%

Figure.1 outlines the Information Security Awareness (ISA) assessment of Social engineering, Policy, and Security Knowledge in company A. The result shows that 30.52% and 39.14 % only know social engineering and policy. In addition, 45.40% know information security when asked about the security Knowledge category. The results indicate that employees' knowledge is low and the company is vulnerable to phishing camping and ransomware which leads to data leakage, and finical ruin.IT employees are a liability to the organization since they need an understanding of how ransomware and social engineering target their target and the tactics, they use to trick their target. According to the interview with the IT department, they claimed they do not have a policy written and they operate with best practices based on their security knowledge. A lack of policy will increase the difficulty to secure the organization for example there are no admin

privileges that will enable users to install and download applications Which makes it easier for threat vectors to install back door or adware. Furthermore, the result shows that the security Knowledge is very low and IT departments are not familiar with information security and security procedures to secure company A. The results indicate that IT departments are not familiar with security procedures and mitigation steps to secure company A. However, they operate according to their self-thought knowledge and best practices they have learned from their experiences. This will enable IT users to operate with security and IT privileges that will lead to one user having over privileges than he is supposed to have. The user will become liable more than reliable because the threat vector focuses on such behavior as to be their next potential prey. The results concluded that the lack of security led to putting the company in serious issues as IT users have the highest privileges in the company system, which makes it easier for hackers to create well-constructed cyber-attack. Additionally, the company needs to invest heavily in a security program to be able to construct threat modeling in the company that will help the company's decision-making when the incident occurs. A company should implement an information security awareness and training program and implement an information security policy that aids in affecting decision-making when an incident occurs.

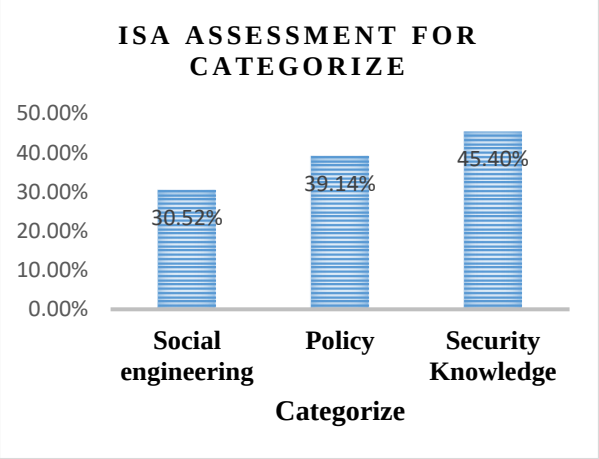

Fig. 1. Social engineering, Policy, and Security Knowledge ɑssessment for IT staff

Table 3 below defines the result of the Security Awareness and Physical security assessment. The result shows only 26% of IT staff undertake security awareness requirements whereas more than half, which is 68%, do not undertake security awareness requirements. In addition, 55.40% follow Physical security procedures while 44.60% unfollow Physical security procedures. The results convey a clear message that there is a lack of security awareness and security awareness requirements in the IT department in Company A

Table 3: Awareness and Physical security ɑssessment for IT staff

Category	Highlight	Percent	
		Yes	No
Awareness	Is the employee aware of the following:	26%	68%
	• Incident report procedures		
	• Company policy		
	• Password policy		
	• Clear disk policy		
Physical security	Availability of the following	55.40%	44.60%
	• CCTV		
	• Log access to the Datacenter		
	• Safety procedure for the data center		
	• Disposing of sensitive data		

Security awareness is an essential part to deal with incidents; Figure.2 summarizes the result of the Information Security Awareness (ISA) assessment of Awareness and Physical security for the IT department in company A. The result shows that only 26% of IT staff know security awareness requirements whereas more than half, which is 68%, do not undertake security awareness requirements. The results show that a lack of security awareness and security awareness requirements which leads to data leakage, and finical loss. The results indicated that the IT department did not take any awareness program to update the employee's knowledge on information security such as (the latest vulnerabilities and how they can secure the organization from threat vectors). In addition, 55.40% follow Physical security procedures while 44.60% un follow Physical security procedures. The result shows that physical security is implemented in a manner to secure the organization. This also indicates that company A is well invested in physical security since the industry in physical security is more developed than in cyber security. However, financial companies need to follow physical security standards to be able to operate in that field. The results concluded that the lack of support from the company board would cause security breaches without being known they got breached. Lack of physical security in the organization increases the possibility of a physical cyber attack using a rubber ducky tool that is capable exploit organization end-user workstations which will lead the threat vector to the organization database or financial application for example for bank SWIFT which will lead to severe loss. A company should be aware of IT staff by implementing information security awareness and training programs and following Physical security policy procedures.

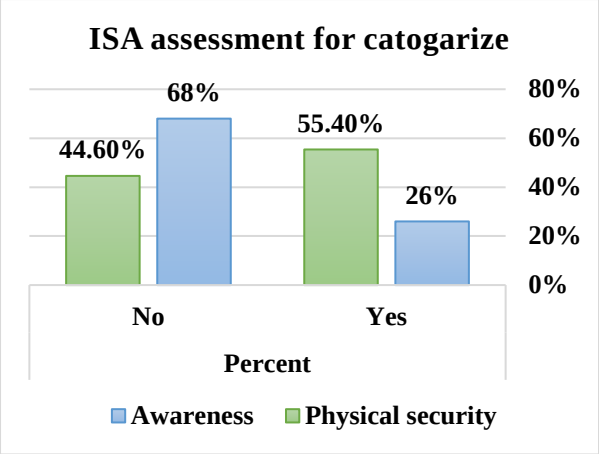

Fig. 2. Awareness and Physical security assessment for IT staff

Table 4 describes the result of the Information Security Awareness (ISA) assessment of Social engineering, Policy, and Security Knowledge for the managers in company A. The result shows that 12.00% and 9.50% know social engineering and policy. In terms of Security Knowledge, the results showed that 14.40% know information security. This indicates that company A managers never have taken or are even familiar with security. Unfortunately, the lack of awareness is a devastating risk to the organization. according to the interview with managers in the company, the privilege they assign requires a good understanding in being aware of the steps needed to be secure from social engineers. Inappropriately, the results show they can be prey to social engineers. So company A needs to issue awareness programs frequently in Social engineering tactics, information security Policy, and Security Knowledge. The results show that there is a need to be aware of Social engineering, Policy, and Security Knowledge in the IT department in company A.

Table 4: Social engineering, Policy, and Security Knowledge assessment for managers

Category	Highlight	Percent
Social engineering	Phishing • Phishing life cycle • Phishing methods • Ransomware	12.00%
Policy	• Segregation of duties • Password policy • strong Password characteristics • organization policy	9.50%
Security Knowledge	• CIA • Vulnerability risk and threat • Security best practices	14.40%

Figure 3 summarizes the Information Security Awareness (ISA) assessment of Social engineering, Policy, and Security Knowledge for managers in company A. The result shows that 12% and 9.50 % only know social engineering and policy. Moreover, 14.40 % only of managers have good knowledge of information security whereas more than half have little knowledge about information security. The results indicate that managers' knowledge is low and the company is vulnerable to phishing camping and ransomware which leads to data leakage, and finical ruin. The results concluded that the majority of managers in company A are not familiar with social engineering tactics or how they can distinguish emails they receive are legitimate or phishing. This makes the company vulnerable to a phishing campaign. That will lead to data leakage and potential breach of the company. The cause of the outrageous drops in the awareness level is that company A does not implement either Policy or awareness program, which dropped the security standard of the organization. In addition, the most targeted group in the organization is the common employee due to a lack of technical and lack of understanding of the importance of the data they acquire. With a lack of policy in the organization that will help end users create shortcuts to complete their daily tasks quickly. Unfortunately, policies have been implemented to create restrictions to avoid security breaches or data leakage. A lack of policy in company A according to the management hierarchy and board is not investing heavily in security which comes with consequences for the organization. Moreover, the results show that company A Lack of security awareness also lack of leadership in security are critical components absent in the organization which makes company A an easy target for threat vectors. Since they are not experienced to discover if the organization is under cyber attack and not capable to mitigate their vulnerability. A company should implement an information security awareness and training program and implement an information security policy that aids in affecting decision-making when an incident occurs.

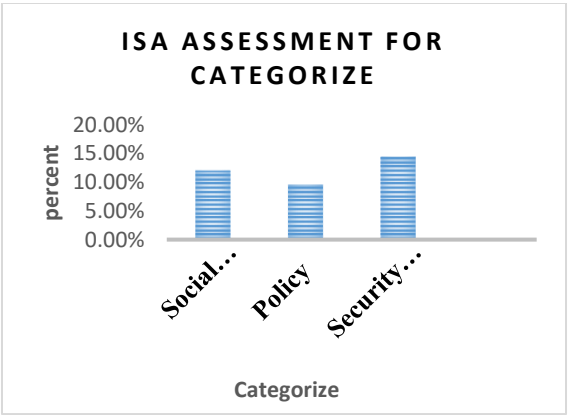

Fig. 3. Social engineering, Policy, and Security Knowledge assessment for managers

4.2 Company B

Table 5 summarizes the result of the Information Security Awareness (ISA) assessment of Social engineering, Policy, and Security Knowledge for the IT department in company B. The result shows that 44.70% and 42.72% only know social engineering and policy. In terms of Security Knowledge, the results showed that 50.80% know information security. The results show that there is a lack of awareness of Social engineering, Policy, and Security Knowledge in the IT department in company B. The data indicates that company results are below average, which is disappointing because the IT manager claimed the organization took more than once online awareness program. Unfortunately, the data shows that the previous online program was ineffective. This study,

recommends providing interactive face-to-face security training programs to identify and educate employees on the gaps.

Table 5: Social engineering, Policy, and Security Knowledge assessment for IT staff

Category	Highlight	Percent
Social engineering	• Phishing • Phishing life cycle • Phishing methods • Ransomware	44.70%
Policy	• Segregation of duties • Password policy • strong Password characteristics • organization policy	42.72%
Security Knowledge	• CIA • Vulnerability risk and threat •Security best practices	50.80%

Figure.4 summarizes the Information Security Awareness assessment of Social engineering, Policy, and Security Knowledge for IT staff in Company B. The result shows that 44.70% and 42.72% recognize social engineering and policy. Furthermore, 50.80% have good knowledge of information security. The results indicate that employees' knowledge is low and the company is vulnerable to phishing camping and ransomware which leads to data leakage, and finical ruin.IT employees are a liability to the organization since they need an understanding of how ransomware and social engineering target their target and the tactics, they use to trick their target. The lack of security will be an advantage to social engineers' favor that enables them to initiate phishing campaigns easily and will be very hard for the IT team to detect or even stop it. However, interview questions showed that they have taken an online awareness program so they should be aware of the risk of cyber-breach. According to the interview with the IT department, they claimed they have a policy written but not authorized by the board and not visible to all employees. That means the policy is only documentation and not implemented across the company. Nevertheless, the reason behind this issue is the lack of a security department and lack of support from the company hierarchy forward securing the company. A lack of policy will increase the difficulty to secure the organization for example there are no admin privileges that will enable users to install and download applications Which makes it easier for threat vectors to install back door or adware. Furthermore, the result shows that the security Knowledge is very low and IT departments are not familiar with information security and security procedures to secure company B, they operate according to their self-thought knowledge and best practices. The main issue is that company B is not investing heavily in security by creating a security department to manage the security in the organization. Security knowledge is considered the highest because the IT department is familiar with cyber security and cyber security defense solution. The results concluded that the lack of security led to putting the company in serious issues as IT users have the highest privileges in the company system, which makes it easier for hackers to create well-constructed cyber-attack. A company should implement an information security awareness and training program and implement an information security policy that aids in affecting decision-making when an incident occurs.

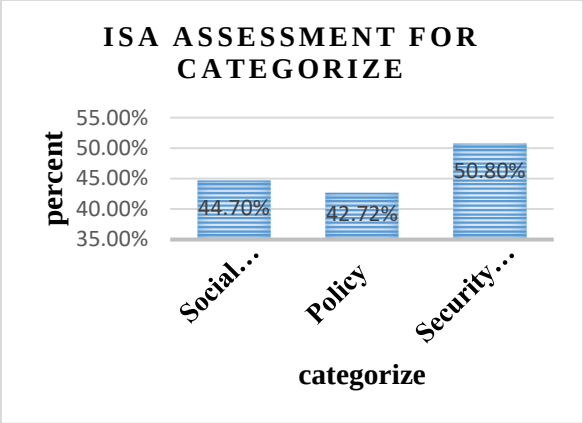

Fig4. Social engineering, Policy, and Security Knowledge assessment for IT staff

Table 6 outlines the result of the Security Awareness and Physical security assessment for the IT department in company B. The result shows that 40 % of IT staff know security awareness requirements while more than half, which is 60%, do not recognize security awareness requirements. In addition, 59.60%follow Physical security procedures while 41.20% unfollow Physical security procedures. The results show that there is a lack of security awareness and security awareness requirements in the IT department in company B. The results find that in the physical security category, only about half of the IT department is aware of the requirements to implement physical security, and about half understands the importance of these procedures which is a very disappointing indication for the IT department. Nevertheless, the results of security awareness are below average which is alarming. Because the IT department in company B acts as the security department that does IT responsibilities and security responsibilities. The summary of results shows that the last line of defense is not capable to comprehend the risk that will cause to company B.

Table 6: Social engineering, Policy, and Security Knowledge assessment for IT staff

Category	Highlight	Percent	
		Yes	No
Awareness	Is the employee aware of the following: • Incident report procedures • Company policy • Password policy • Clear disk policy	40%	60%
Physical security	Availability of the following • CCTV • Log access to the	59.60%	41.20%

	Datacenter • Safety procedure for the data center • Disposing of sensitive data		

Figure.5 outlines the result of the Security Awareness and Physical security assessment for the IT department in company B. The result shows that 40 % of IT staff recognize security awareness requirements whereas more than half, which is 60%, do not know security awareness requirements. The results show that a lack of security awareness and security awareness requirements which leads to data leakage, and finical loss. The results indicated that there is a lack of security awareness and security awareness requirements in the IT department in company B. Moreover, interview questions showed that they have taken an online awareness program. In addition, 59.60% follow Physical security procedures while 41.20% unfollow Physical security procedures. The result shows that physical security is implemented in a manner to secure the organization. This also indicates that company A is well invested in physical security since the industry in physical security is much faster than in cyber security. However, financial companies need to follow physical security standards to be able to operate in that field. The results concluded that the lack of support from the company board would cause security breaches without being known they got breached. A company should be aware of IT staff by implementing information security awareness and training programs and following Physical security policy procedures.

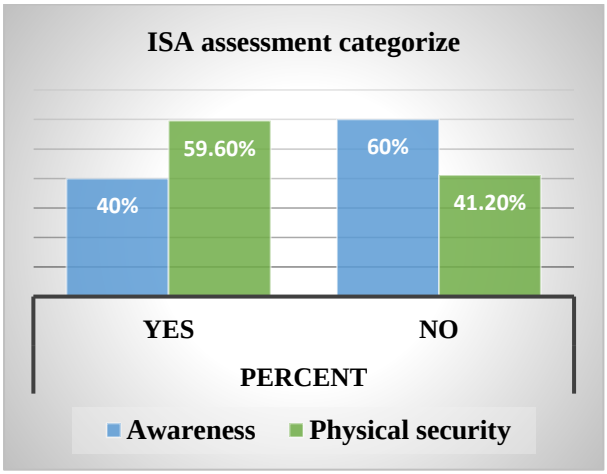

Fig. 5. Awareness and Physical security assessment for IT staff

Table 7 describes the result of the Information Security Awareness (ISA) assessment of Social engineering, Policy, and Security Knowledge for the managers in company B. The result shows that 20%and 23.00% know social engineering and policy. In terms of Security Knowledge, the results showed that 15.00% know information security. The results show that there is a need to aware of Social engineering, Policy, and Security Knowledge for managers in company B. the results show that the most targeted user in the organization is not aware of the risk that a remonstrance attack can impact the company B. also they are not familiar with the procedure needed to operate there task without compromising the organization.

Table 7: Social engineering, Policy, and Security Knowledge assessment for managers

Category	Highlight	Percent
Social engineering	• Phishing • Phishing life cycle • Phishing methods • Ransomware	20%
Policy	• Segregation of duties • Password policy • strong Password characteristics • organization policy	23.00%
Security Knowledge	• CIA • Vulnerability risk and threat • Security best practices	15.00%

Figure.6 summarizes the Information Security Awareness assessment of Social engineering, Policy, and Security Knowledge for managers in company B. The result shows that 20% and 23.00% know social engineering and policy. Moreover, 15.00 % only of managers have good knowledge of information security whereas more than half have little knowledge about information security. The results indicate that managers' knowledge is low and the company is vulnerable to phishing camping and ransomware which enable social engineers to breach company B easily due to a lack of understanding of the risk of cyber malware or the techniques the social engineers use. However, the risk of being compromised is not only financial but also the reputation of the company which can lead to severe loss. The results show that company B never shared policies or procedures that need to be taken when an incident occurs however, the IT department implants technical procedures (active directory) to access and manage the users in the organization. Nevertheless, the result shows that twenty percent of the employees understand the characteristics needed to have a strong password. The main cause of this issue is a lack of awareness and the users' does not understands the importance of the data they acquire. In addition, a lack of policy in the organization that will help end users create shortcuts to complete their daily tasks quickly. Unfortunately, policies have been implemented to create restrictions to avoid security breaches or data leakage. A company should implement an information security awareness and training program and implement an information security policy that aids in affecting decision-making when an incident occurs. Furthermore, focus on implementing the awareness program at least twice a year to cope with the latest cyber-attack.

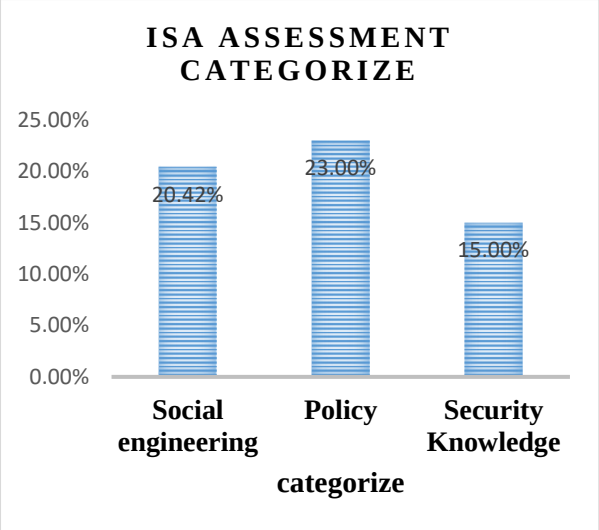

Fig6. Social engineering, Policy, and Security Knowledge assessment for managers

Table 8 outlines the Security Awareness and Physical security assessment for the managers in company B. The results show that 37.20%of managers recognize security awareness requirements whereas more than half, which is 62.80%, do not know security awareness requirements. Additionally, the results show that 45% follow Physical security procedures while 55% unfollow Physical security procedures. The results find that the previous awareness program for company B was ineffective for the managers because the level of understanding of the risk of cyber attack is not clear to many employees. This can lead to irresponsible behavior that can lead to consequential actions on company B. The physical security results are very disappointing because the physical security culture is already known in the financial organization. The process and procedure should be known to all members of the organization however the managers are not familiar that hackers can exploit the organization using physical hacking tactics they believe threat vectors operate remotely only which is accurate. The results concluded that there is a lack of security awareness and security awareness requirements for managers in company B.

Table 8: Awareness and Physical security assessment for r managers

Category	Highlight	Percent	
		Yes	NO
Awareness	Is the employee aware of the following:	37.20%	62.80%
	• Incident report procedures		
	• Company policy		
	• Password policy		
	• Clear disk policy		
Physical security	Availability of the following	45%	55%
	• CCTV		
	• Log access to the Datacenter		
	• Safety procedure for the data center		
	• Disposing of sensitive data		

Figure.7 summarizes the result of the Security Awareness assessment and Physical security for the IT department in company B. The result shows that only 37.20% of managers recognize security awareness requirements whereas more than half, which is 62.80%, do not know security awareness requirements. The results indicated that there is a lack of security awareness and security awareness requirements for company managers. Moreover, interview questions showed that they have taken an online awareness program. Results show that company B invests in awareness to educate employees of the risk of cyber-attack and social engineers. However, lack of consequences for employees who do not intend to follow the guideline been taking in the awareness program. This is Lead to a breach of the policy without an entity implementing consequences actions reactions to employees who violate policies and procedures that they took in the awareness program. In addition, 45% follow Physical security procedures while 55% unfollow Physical security procedures. The result shows that physical security is implemented in a manner to secure the organization. This also indicates that company B is well invested in physical security since the industry in physical security is much faster than in cyber security. However, financial companies need to follow physical security standards to be able to operate in that field. The results concluded that company B invests in awareness to educate employees of the risk of cyber-attack and social engineers. However, lack of consequences for employees who do not intend to follow the guideline been taking in the awareness program. This is Lead to a breach of the policy without an entity implementing consequences actions reactions to employees who violate policies and procedures that they took in the awareness program. Thus, this behavior will enable users to operate without restrictions for example using Removable media to move data around the network, which can lead to a ransomware attack. Assessment results find that the awareness program of Company B is ineffective, the results indicate that managers have low knowledge of security procedures and a decent knowledge of physical security requirements. This data illustrates that company B either lacks security experience and they have not invested in the organization's security gap. However, the results are alarming that will cause severe loss to the organization if the right procedures are not implemented. A company should be aware of managers by implementing information security awareness and training programs and following Physical security policy procedures.

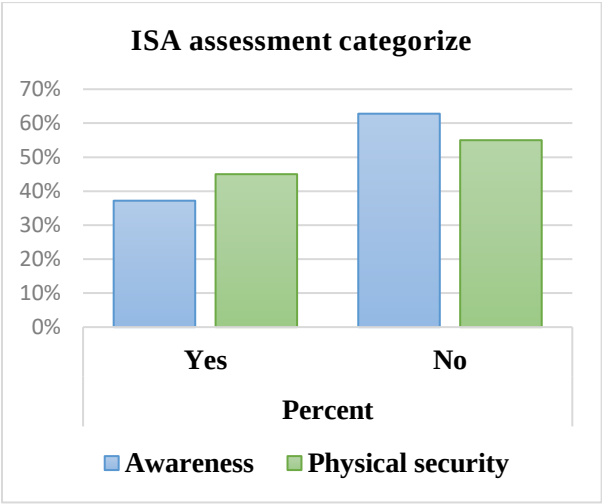

Fig. 7. Awareness and Physical security assessment for managers

5. CONCLUSION

The fast growth of information technology has made it simpler, more accurate, and more efficient to carry out organizational purposes. However, there is still a gap between how far technology has advanced and how much employees are aware of it, making it challenging for privet financial organizations to protect their assets. A lack of ISA causes many security risks and challenges. 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 s 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 be managed in the Bank. The risk identification process and documentation as well as control mechanisms are unsystematic. in addition, companies do not implement a formal well-defined information security policy and its derivatives (guideline, Procedure, and Standard) that give guidance and direction to all members and stakeholders of the companies regarding the management and protection of information assets. Thus, the lack of proper information security policy and guideline implementation in the companies is a critical area for improvement.

6. RECOMMENDATIONS

- The companies 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.
- The companies should implement an information security policy that gives guidance and directions to all members of the companies regarding the management and protection of information assets. The policies should provide direction for the implementation of the other information security components and must be implemented in the organization using effective processes that also include awareness training, compliance monitoring, and auditing thereof.
- Management of the companies should construct the information security department at the higher possible level in the organization and take the information security agenda as an important performance measurement and should commit enough resources for the operation of information security in the companies.
- The companies should compile and implement a formal and well-defined business continuity and disaster recovery document that gives guidance and direction to all members and stakeholders of the company regarding the management and protection of information assets during disasters.
- Information security awareness program requires to be updated in parallel with the change in the business environment in the companies.

7. REFERENCES

[1] Blythe, J. 2013. Cyber security in the workplace: Understanding and promoting behavior change. In Proceedings of CHItaly Doctoral Consortium, 92-101.

[2] He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L., and Tian, X., 2019. Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. Journal of Intellectual Capital.

[3] Bulgurcu, B., Cavusoglu, H., and Benbasat, I.2010. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly. 34(3), 523-548.

[4] Watters, P. A., and Ziegler, J.2016. Controlling information behavior: the case for access control. Behavior & Information Technology. 35(4), 268-276.

[5] Hina, S., and Dominic, D. D.2018. Information security policies' compliance: a perspective for higher education institutions. Journal of Computer Information Systems. 60(3), 1-11.

[6] Johnson, M. E., and Goetz, E. 2007. Embedding information security into the organization. IEEE Security & Privacy, 5(3).

[7] Li, L., He, W., Xu, L., Ash, I., Anwar, M., and Yuan, X. 2019. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management.Vol 45, 13- 24.

[8] Accenture. 2019. Cost of Cybercrime, Study. https://www.accenture.com/us-en/insights/security/costcybercrime-study

[9] Adam, A., Catherine, G., Edison, W. 2023. Factors Affecting the Security of Information Systems: A Literature Review. The International Journal of Engineering and Science (IJES). Vol10 (1), 57-65.

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

[11] Salima, B., and Abdelfattah, M.2019. Wireless Security in Libya: A Survey Paper. International Journal of Computer Applications. 181(35),26-31.

[12] Shanfari, A.l., Warusia, Y., Nasser, T., Roesnita, I. and Anuar, I.2022. Determinants of Information Security Awareness and Behavior Strategies in Public Sector Organizations among Employees. (IJACSA) International Journal of Advanced Computer Science and Applications. Vol. 13(8).

[13] Emad, S. 2022.Vulnerability of Saudi Private Sector Organizations to Cyber Threats and Methods to Reduce the Vulnerability. Pertanika J. Sci. & Technol. 30 (3): 1909 - 1926.