DOI: http://dx.doi.org/10.26483/ijarcs.v14i5.7021

ISSN No. 0976-5697

Volume 14, No. 5, September-October 2023

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

SECURITY ISSUES IN LIBYAN GOVERNMENT COMPANIES

Salima Benqdara
Computer Science,University of Benghazi
Benghazi, Libya

Abstract: The growth of technology, communications, and the cyber-Internet has led to a revolution in how data and information are sent and used online. As a result, internet security has become a crucial concern, particularly in safeguarding sensitive data in the government company. Government company a vital infrastructure for modern society, is also a lucrative target for cyber attacks, which could potentially expose sensitive customer information. This study highlights the importance of internet security in safeguarding sensitive data in government companies such as telecommunications companies. The study conducted in Libya employed an interview technique to evaluate the information security policy of government companies and identified several vulnerabilities that require mitigation to protect networks from cyber attacks. The study emphasizes the significance of information security in government companies and provides insights that can assist companies in developing and implementing effective policies to safeguard their networks.

Keywords: Information security, policy Implementation Assessment, information security management

I. INTRODUCTION

Telecommunications services have undergone a significant revolution in recent years, making the world more interconnected than ever before. With the rise of telecommunications services such as healthcare providers, law enforcement agencies, and banks, these services have become essential to the majority of people worldwide. They form the backbone of modern civilization, and people, organizations, and governments rely heavily on them to provide public services and exchange basic services via the Internet. Any disruption to these services can result in significant losses. Moreover, telecommunications organizations maintain detailed databases of their customers, making them a lucrative target for cyber attacks. If such a database is exposed to a third party, it can pose a significant risk to both the user and the service provider. Hence, these organizations need to have a robust information policy to safeguard their networks and protect their customers' data [1].

The significance of information security in any organization cannot be overstated. It safeguards data resources and ensures the confidentiality, integrity, and availability of data, which are the three foundational pillars of data security. Due to the increasing rate of threats against information technology infrastructure worldwide, information security issues persist in organizations, including data breaches, systems outages, and malicious software. To control users' security-related behavior, organizations need a platform and environment of regulations, which is provided by an information security policy. Policies direct how issues should be addressed and what technologies should be used. However, policies do not specify the proper operation of equipment or software, which should be placed in the standards, procedures, and practices of users' manuals and systems documentation. It is crucial to ensure that policies do not contradict the law, as this can create significant liability for the organization [2]. While security policies are the least expensive control to execute, they are the most difficult to implement properly. Therefore, organizations must ensure that their information security policies are well-formulated, regularly updated, and effectively communicated to all users to safeguard their data resources and protect against cyber threats.

Threats to information security can arise from various sources, including policy issues, policy implementation issues, and employees' security-related behavior. The human aspect of information security is a critical and challenging component in creating a safe and secure information environment [3]. A survey by the Computer Security Institute revealed that insider security-related abuse is the second-most frequently occurring computer security incident, with an average monetary loss of $288,618 per incident [4]. In the absence of a strong and properly formulated information security policy, it becomes much more difficult to control or punish employees' security-related behavior. The expected severity of such a situation is catastrophic to any organization, given that up to 80% of major security breaches in an organization result from employees' incorrect behavior rather than technical weaknesses in information systems [5]. The information systems (IS) security literature highlights a growing interest in investigating employee behavior that may have security implications in organizations [6]. In line with this, firms and organizations should adopt similar growth in policy adoption to mitigate the consequences of such behavior. By implementing effective information security policies and providing regular training to employees, organizations can create a strong security culture that can reduce the risks posed by human factors and protect against insider threats. the importance of information security policies in mitigating the risks posed by human factors cannot be overstated. Organizations must prioritize the human aspect of information security and ensure that their policies are well-formulated, regularly updated, and effectively communicated to all employees. The implementation of effective policies and regular training can create a strong security culture in organizations, reducing the risks posed by insider threats and ensuring the safety and security of sensitive information.

This paper has proposed to assess the information security procedure of government companies in Libya. The objective of this study is to assess the hypothetical risks of the implementation of an information security procedure as well as to examine the vulnerabilities and effectiveness of that procedure. 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

II. RELATED WORK

In 2016, Alshaikh et al. constructed a model for managing information security policy that encompasses three stages of institutionalization: development, implementation and maintenance, and evaluation. Each stage comprises various management practices, with a focus on exploring the relationship between these practices and information security policy in organizations. The study identified several limitations that hinder organizations' ability to effectively implement security policy through managerial practices. The study provides valuable insights into the challenges faced by organizations in managing information security policies. By dividing the process into three distinct stages, the model offers a structured approach to policy implementation and evaluation. The study's identification of shortcomings in managerial practices highlights the importance of addressing these issues to ensure the successful implementation of security policies. Overall, this research contributes to the development of effective strategies for information security procedure management, which is crucial in today's increasingly digital world.

In 2019, Ključnikov et al. conducted a study to identify the factors that contribute to successful information security management in small and medium enterprises (SMEs) in Slovakia. The findings revealed that the application of security controls, such as the implementation of standards, technical and procedural measures, and risk management, were key indicators of successful information security management. The second most important factor was found to be supportive top management. The study recommends that SMEs prioritize organizational awareness regarding information security management alongside the implementation of security controls as the first line of defense to protect their valuable information assets. By doing so, these companies can ensure that their information remains secure and protected from potential threats. The research conducted by Ključnikov et al. sheds light on the importance of having a comprehensive approach to information security management in SMEs, which can ultimately lead to their long-term success and sustainability in today's digital landscape.

A study conducted by Al-Izki and Weir in 2016 examined management attitudes toward Information Security in Oman and its impact on Information Security governance. The researchers aimed to assess the current level of compliance with Information Security procedures in public sector organizations in Oman, analyze management attitudes towards Information Security governance practices, and investigate how these attitudes influence various aspects related to Information Security. The findings of the study indicated a significant lack of interest from management in Information Security within Omani public sector organizations. This implies that Information Security was not given due importance and attention at the management level. Additionally, the results revealed a strong correlation between management attitudes toward Information Security and indicators of management governance activities. This suggests that how management perceives and values Information Security has a direct impact on the implementation and effectiveness of Information Security policies and practices. In conclusion, the study established a robust relationship between management attitudes toward Information Security and compliance with Information Security policies. In other words, when management demonstrates a positive and proactive attitude toward Information Security, it leads to higher levels of compliance with Information Security policies within the organization. This highlights the critical role of management in fostering a culture of Information Security and ensuring the organization's adherence to Information Security standards. Overall, the study emphasizes the significance of management attitudes in shaping Information Security governance and underscores the need for management to prioritize and actively support Information Security initiatives within Omani public sector organizations.

Salima et al. (2020) proposed a framework aimed at assessing information security issues in Libyan banks. The study sought to evaluate the security strategy in these banks and identify any security gaps. To achieve this objective, the researchers collected data by conducting interviews with information security staff to assess the current security strategy in Libyan banks. The study collected data on the current security situation in selected banks in Libya. The collected data were then analyzed using a risk assessment matrix and a static tool to identify critical assets that required protection. During the data analysis process, vulnerabilities were mapped to potential threats, and the impact of these threats on security characteristics was assessed. The study determined the Confidentiality, Integrity, and Availability (CIA) of the banks' information based on the probability and impact of the identified security flaws. The findings revealed that the current security flaws mainly affected the availability and confidentiality of the banks' information. It was also observed that there was no standard deployment in information security management, and each bank had the freedom to choose the appropriate standards for their operations. The study identified security gaps in the existing security system, particularly in the sharing of customer information in response to their requests. In conclusion, the study recommended that information security management in Libyan banks should enhance its processes and be mindful of the benefits and advantages associated with adopting information security standards. Furthermore, the researchers suggested that Libyan banks should implement a comprehensive and adequate set of information security components to address threats at technical, process, and people levels. This should be based on the identified information security risks and the appropriate controls necessary to mitigate these risks.

Carvalho et al. (2018) conducted a study to identify the most important and least relevant elements in the structure of a security policy. They synthesized existing literature on information security policy content and characterized 15 Small and Medium-Sized Enterprises (SMEs). The researchers used content analysis (CA) as a research technique to analyze and describe information security policies. The study revealed that the relative importance of these elements varied slightly depending on the sectors of activity. The findings emphasize the need for SMEs to be aware of these elements to design their security policies in a precise, concise, and unambiguous manner.

Al-Shanfari et al. (2022) proposed a comprehensive theoretical model based on the Protection Motivation Theory to assess employees' intentions for information security behavior. The study employed a survey and structural equation modeling (SEM) to analyze the data. The research indicated that risks and behaviors should influence awareness efforts, emphasizing the importance of providing employees with Information Security Awareness (ISA) programs and continuously evaluating their effectiveness. The research model was extended to include facilitating conditions that ensure actual adherence to information security regulations and policies.

Alkhurayyif et al. (2017) investigated the effectiveness of applying readability metrics as indicators of policy comprehensibility. The study focused on assessing readability factors that affect the success and effectiveness of Information Security Policies (ISPs). The preliminary study demonstrated variations in comprehension test results due to the difficulty of the policies examined. There was a correlation between software readability and human comprehension test results, suggesting that readability impacts understanding of ISPs. The findings have implications for users' compliance with information security policies and suggest the use of readability metrics to evaluate draft policies for ease of comprehension before release. This supports the potential for a readability compliance test for future ISPs.

Rathika et al. (2022) conducted a literature review to gather evidence related to the risk of non-compliance with security policies in employee behavior and mitigation strategies. The review mapped the risks according to the People, Process, and Technology (PPT) Model. The study found that security policy compliance in a Bring Your Device (BYOD) environment is still inconsistent. In their literature review, Rathika et al. (2022) aimed to collect evidence regarding the risks associated with non-compliance with security policies in employee behavior and explore potential mitigation strategies. They utilized the People, Process, and Technology (PPT) Model to map the identified risks. The study specifically focused on compliance with security policies in a Bring Your Device (BYOD) environment. The findings of the review indicate that security policy compliance in a BYOD setting is still inconsistent. This suggests that employees using their devices for work-related tasks may not consistently adhere to the organization's security policies. Non-compliance with security policies poses significant risks to the confidentiality, integrity, and availability of sensitive information and can potentially lead to security breaches and data loss. The inconsistent compliance with security policies in a BYOD environment can be attributed to several factors. Firstly, employees may not fully understand the importance of adhering to security policies when using their devices for work purposes. Secondly, there may be a lack of clear guidelines and communication regarding security expectations and requirements for BYOD usage. Thirdly, employees may perceive security measures as burdensome or inconvenient, leading to non-compliance.

III. PROPOSED APPROACH

In this research study, a government company was selected as the case study. The information security policy (ISP) of this company was thoroughly examined and found to be optimal, regularly updated, and aligned with international information standards. However, during the investigation, it became apparent that there were certain issues in the implementation of the ISP within the organization. To delve deeper into the implementation process, the research employed the Interview Method, focusing specifically on the managerial level responsible for the implementation. The process of the proposed approach is as follows:

Data Collected

The data collection process involved conducting qualitative research through interviews with managers in the organization. The interviews were thoughtfully designed to address the managerial aspects of ISP implementation. The interview structure provided ample space and freedom for the interviewed personnel to express their thoughts and ideas on the subject matter. The interview questions were prepared in advance and categorized into seven distinct areas, as indicated in Table 1.

Table 1: Mapping interview questions to interview aspects

	Factor	***Question***	***Highlight***
1	Awareness with ISP	Q1	awareness with ISP in the organization
2	Enforce policy	Q2	enforce policy in the organization
3	Roles and Responsibility	Q3	roles and responsibilities in general regarding the ISP in the organization
4	Attitude and compliance	Q4	Attitude and point of view toward compliance with the ISP
5	Aware of disciplinary penalties	Q6	Aware of disciplinary penalties for noncompliance behavior with the information security policy in the organization

DATA ANALYSIS

Once the data and information are collected, the next step is data analysis. In this study, a risk assessment analysis is conducted to evaluate the current status of the security strategy. This analysis involves interviewing the managers of the company and identifying any security gaps that exist in the current situation.

RISK ASSESSMENT

To assess the risks, a risk matrix is utilized as a risk assessment technique. The risk matrix considers the severity or impact of a particular aspect against its probability or likelihood. This approach aligns with the recommendation made by Mr. Mohan Kamat during his contribution to the

ISO 27001 Implementer's Forum in 2009 [6]. The risk matrix provides a simple mechanism to visualize and understand the risks, aiding management decision-making processes. The figure below illustrates the risk matrix that was employed in this study.

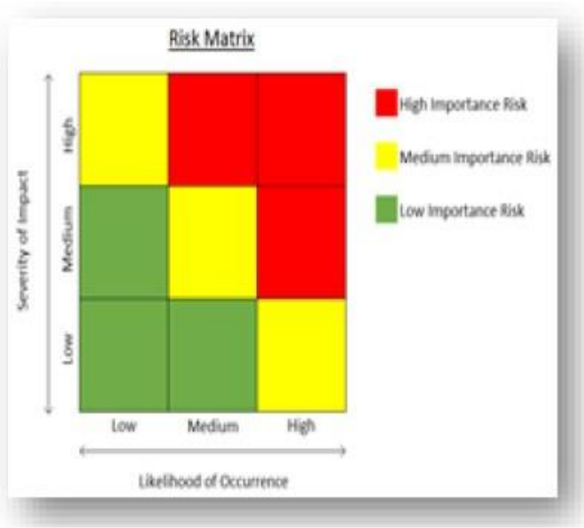

Figure 1 Risk matrix

IV. EXPERIMENTAL SETUP

The experimental setup in this section consists of two main parts. Firstly, the current situation is analyzed by identifying the security gaps based on the analyzed data. Secondly, a risk matrix is utilized for risk assessment to determine the level of risk. The risk matrix considers the category of probability or likelihood and compares it to the category of consequence severity. This approach allows for a comprehensive understanding of the risk levels involved.Using the Template

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper.

V. RESULTS AND DISCUSSION

A-Factor 1 Awareness with ISP

The presented Table highlights a concerning situation regarding the knowledge and awareness of the entity's ISP within the government company. The information presented in Table 2 indicates that the employees of the government company have a limited understanding of the entity's Information Security Policy (ISP), and the managers are not well-informed about the details and updates of the ISP. This lack of knowledge and awareness poses a significant risk to the confidentiality, integrity, and availability of the company's information. Moreover, the policy itself is deemed unrealistic, which diminishes its effectiveness and the overall security standards within the organization. Consequently, this situation increases the likelihood of potential cyberattacks. The absence of an awareness program and the failure to implement the information security policy have played a role in the company's inability to identify information security risks adequately and establish appropriate security standards. To address these issues, the company should invest substantially in a comprehensive security program. Such a program would enable the construction of threat models that facilitate decision-making during security incidents. Therefore, the company must implement a security awareness program to enhance understanding and awareness of the security policy among its employees. The insights derived from Figure 2 underscore the necessity for the company to take proactive measures to enhance its security posture. Employees' limited knowledge of the ISP and managers' lack of awareness regarding its details and updates imply that employees may not be taking sufficient measures to safeguard the company's information, while managers may not be up to date with the latest security threats and vulnerabilities. Moreover, the unrealistic nature of the policy further undermines its impact and the overall security standards. Poorly implemented or impractical policies can create security gaps and increase the organization's overall risk of cyberattacks. To address these issues, Regular assessments and audits can help identify and address any implementation gaps. Additionally, companies should stay updated on emerging threats and regularly review and update their policies and security standards to address new risks effectively. In conclusion, the findings suggest that the company should prioritize improving knowledge and awareness of the security policy, implement realistic and practical security measures, and invest in a comprehensive security program that includes threat modeling. These steps will help reduce the risk of cyber-attacks and protect the company's valuable information assets.

Table 2. Risk evaluation awareness with ISP in the government company

Probability	***Effect on***			***Risk evaluation***	***Consequences***
	C	**I**	**A**	**Significant Risk**	• negative effects on confidentiality , integrity, and availability • The policy will be impractical, decreasing its impact and the security standard in the organization • Increased risk of cyberattacks
High	✓	✓	✓		
Medium					
Low					

B- Factor 2 Enforce policy in the government company

Table 3 presents a summary of the enforcement policy in the government company. The table shows that the company has a high risk of confidentiality and integrity breaches. This situation can be attributed to several factors, including the absence of an enforcement policy, a lack of security expertise within the company, and inadequate employee training on information security. The absence of an enforcement policy means that there is no clear plan in place for responding to security incidents or mitigating risks.

This can result in delayed incident responses, making containment more challenging. Moreover, the absence of an enforcement policy makes it difficult to hold employees accountable for security breaches. Furthermore, the lack of security expertise within the company means that there is a lack of individuals with the necessary skills and knowledge to develop and implement a comprehensive security program. Consequently, security vulnerabilities may go undetected and unaddressed. Additionally, the lack of security expertise hinders effective incident response. Another contributing factor is the insufficient training provided to employees regarding information security. Without proper training, employees may be unaware of the risks they face and the steps they should take to safeguard the company's information.

This can lead to inadvertent mistakes by employees that compromise the company's security. The result findings that the company needs to improve its security posture. Employees' limited knowledge of the ISP and managers' lack of awareness regarding its details and updates indicate that employees may not be taking adequate measures to protect the company's information, while managers may not be up to date with the latest security threats and vulnerabilities. Additionally, the unrealistic nature of the policy diminishes its impact and the overall security standards in the organization, increasing the risk of cyberattacks. To address these issues, the company should consider implementing a comprehensive security awareness program. This program will enable the company to reduce the risk of security breaches and protect its valuable information. By improving employees' knowledge and awareness of the security policy, the company can foster a culture of security consciousness and empower employees to take proactive steps in safeguarding company data.

Table 3. Risk evaluation for enforcing policy in the government company

Probability	*Effect on*			*Risk evaluation*	*Consequences*
	C	**I**	**A**	**High Risk**	- Negative effects on confidentiality and integrity - The lack of security experience in the department will impact heavily in handling mitigation procedures and constructing secure defense for the organization.
High	✓	✓			
Medium			✓		
Low					

Sample of a Table footnote. (Table footnote)

•C- Factor 3 - Roles and Responsibilities in general regarding the ISP

Table 4 provides an overview of the roles and responsibilities within the Government Company regarding the Information Security Policy (ISP). The Table reveals a high-risk impact on the confidentiality and integrity of information. Due to the significant impact on confidentiality and integrity, as well as the increased risk of irresponsible behavior and becoming a target for threat vectors, the risk score for this risk is high.

The results indicate that the management team's involvement in the ISP is minimal and passive, suggesting a lack of active engagement in setting and enforcing the policy. This lack of management involvement raises concerns because the management team holds ultimate responsibility for the security of the company's information. The management team's role in ISP tasks is limited, with occasional direct instructions being provided. This situation is partially attributed to a lack of knowledge, specialization, and clearly defined job descriptions. The lack of necessary knowledge or experience in setting and enforcing the ISP further contributes to the issue. Additionally, the absence of explicit responsibilities for information security in the management team's job descriptions compounds the problem. The results also highlight the lack of segregation of duties within the organization. This means that the company lacks a system to separate different duties and responsibilities, which increases the risk of irresponsible behavior and provides users with excessive privileges. Such a situation poses a risk to the organization and makes employees more vulnerable to threat vectors. Due to the significant impact on confidentiality and integrity, as well as the increased risk of irresponsible behavior and becoming a target for threat vectors, the risk score for this risk is high. By addressing these issues and taking proactive measures, the company can strengthen its information security posture, improve management involvement in ISP tasks, and establish clear responsibilities throughout the company. This will contribute to a more secure environment and reduce the risk of security breaches.

Table 4. Risk evaluation for Roles and Responsibilities in the government company

Probability	*Effect on*			*Risk evaluation*	*Consequences*
	C	**I**	**A**	**High Risk**	- Lack of segregation duties will enable irresponsible behavior from the organization by providing over privileges to users which makes them a risk to the organization and a target for threat
High	✓	✓			
Medium			✓		
Low					

					vector • Difficulty in Detecting and Investigating Security Incidents

- ***D- Factor 4 Attitude and compliance with the ISP Significant***

Table 5 highlights the attitude and perspective toward compliance with the Information Security Policy (ISP) within the government company. The results indicate a significant impact on confidentiality, integrity, and availability of information. The failure to comply with the ISP and the resulting negative effects on confidentiality, integrity, and availability of information can indeed have serious consequences. This risk can lead to breaches of confidential information, compromised integrity of data, and disruptions in availability. The results reveal that managers generally have no intention to be non-compliant with the ISP under normal circumstances. However, they may resort to non-compliance as an exception when they perceive no other way to carry out their job responsibilities. One example provided is a manager who, while on vacation outside the country, was unable to access their job's account remotely via a VPN. In this situation, the manager gave their access credentials (username and password) to a colleague to accomplish an urgent task locally. The manager acknowledges that this behavior is both illegal and insecure, but they see it as the only way to complete the task promptly. Such behavior is unprofessional and irresponsible, creating a vulnerability that can make the organization a target for social engineering attacks. The lack of management involvement in setting and enforcing the ISP is a serious issue because it indicates that the management team is not prioritizing the security of the company's information. As the ultimate responsibility for information security lies with the management team, their active engagement in setting and enforcing the ISP is crucial to protect the company from security breaches. Furthermore, the absence of segregation of duties poses risks where employees have access to systems and data sets beyond what their job responsibilities necessitate. This increases the likelihood of unauthorized activities, such as fraud. For instance, an employee with access to both financial records and customer databases could potentially manipulate financial data and exploit customer information for fraudulent purposes. To mitigate this risk, organizations should implement segregation of duties controls that restrict employees' access to only the information and systems required for their specific tasks. This can be achieved by assigning different employees to different responsibilities and implementing access controls accordingly. Segregation of duties is an important control to protect organizations from fraud, errors, and other security risks. Additionally, the company should consider hiring a qualified security professional to assist in developing and implementing an information security program. A security professional can assess and mitigate security risks, identify vulnerabilities, develop appropriate controls, and provide training to employees on safeguarding the company's information. Regular security audits should also be conducted to identify any weaknesses or vulnerabilities in the information security program. Security audits help in assessing the effectiveness of controls and enable the company to address any identified vulnerabilities before they can be exploited. By prioritizing management involvement, providing adequate training, raising awareness about the potential risks and consequences, establishing clear guidelines and consequences for non-compliance implementing segregation of duties controls, hiring security professionals, and conducting regular security audits, the company can enhance its information security posture, mitigate risks, and ensure the protection of its sensitive data and systems.

Table 5. Risk evaluation for Attitude and compliance in the government company

Probability	***Effect on***			***Risk evaluation***	***Consequences***
	C	**I**	**A**		
High	✓	✓	✓	**Significant Risk**	•Overall negative effects on confidentiality, integrity, and availability are significant. Engaging in such unprofessional and irresponsible behavior identifies the organization as a potential target for social engineering attacks. •policy suffers from a lack of enforcement and inconsistent auditing. As a result, the security standard is compromised, leading to potential chaos within the organization and increasing the risk of cyber attacks.
Medium					
Low					

- ***E- Factor 5 Aware of disciplinary penalties for non-compliant behavior***

Table 6 highlights the summary of employees' awareness of disciplinary penalties for non-compliant behavior with the Information Security Policy (ISP) within the government company. The table indicates a significant risk impact on confidentiality, integrity, and availability of information resulting from this lack of awareness. The lack of awareness regarding the security policy can have significant negative effects on the organization's confidentiality, integrity, and availability of information. Confidentiality may be compromised if employees are unaware of how to handle sensitive data properly, leading to unauthorized access or disclosure. Lack of awareness can also result in unintentional or deliberate actions that compromise the integrity of data, such as unauthorized modifications or deletions. Moreover, availability may suffer if employees are not aware of the potential risks and preventive measures, increasing the likelihood of system failures or disruptions. The results show that employees are generally aware of the potential risks associated with non-compliance with the ISP. However, they lack awareness of the specific disciplinary penalties that may be imposed for non-compliance. This lack of knowledge can lead to irresponsible behavior, as employees may not perceive any significant consequences for non-compliance. Although there have been isolated cases of disciplinary penalties imposed for non-compliance, these instances have been rare. This suggests that the company may not be taking information security seriously enough, and employees may not believe that there are real repercussions for non-compliance. The results find that a lack of awareness can result in irresponsible behavior that makes the organization a target for various threat vectors. Furthermore, the absence of consequences or penalties within the organization contributes to disciplinary issues. This, in turn, impacts the severity of vulnerabilities within the organization, as individuals may not take security measures seriously if there are no repercussions for non-compliance. To mitigate this risk, the company must prioritize security awareness and education, ensuring that employees understand the significance of the security policy. Implementing appropriate consequences for non-compliance and addressing disciplinary issues promptly can help deter irresponsible behavior and improve the overall security posture of the organization.

Table 6. Risk evaluation for Attitude and compliance in the government company

Probability	***Effect on***			***Risk evaluation***	***Consequences***
	C	**I**	**A**		
High	✓	✓	✓	**Significant Risk**	•Overall negative effects on confidentiality, integrity, and availability can be significant when there is a lack of awareness regarding the importance of the security policy within the organization. • This lack of awareness can result in irresponsible behavior that makes the organization a target for various threat vectors. •absence of consequences or penalties within the organization contributes to disciplinary issues which will impact vulnerability severity in the organization's
Medium					
Low					

- ***F- Comparison of the risk effect on the factors***

Figure 2 represents the estimated risk impact of each element on the three components of the CIA triad (confidentiality, integrity, and availability). The findings reveal that the government company faces a high risk of security breaches in all three areas. This implies that there is a significant likelihood of unauthorized disclosure of information, unauthorized modifications, or unavailability of critical data when needed. The study identifies issues in the implementation of the Information Security Policy (ISP) within the company, leading to a lack of enforcement and inconsistent auditing of the policy. Consequently, this can result in a lowered security standard overall and create chaos within the organization, potentially leading to cyber attacks. The study concludes that the company would benefit from the proper implementation of its ISP. It is recommended that the company focuses on the factors identified in the government organization. To address the problems highlighted in Figure 2, the company should prioritize increasing awareness of the importance of the security policy among its employees, ensuring consistent enforcement of the policy, and fostering a culture of security throughout the organization. Additionally, the study suggests that the government organization company needs to take specific steps to enhance its information security posture. This includes implementing robust security controls such as encryption, access control mechanisms, and intrusion detection systems. Furthermore, employee training on security best practices should be conducted, and regular security audits should be performed to proactively identify and mitigate vulnerabilities. By undertaking these measures, the company can effectively reduce the risk of security breaches and safeguard its valuable data.

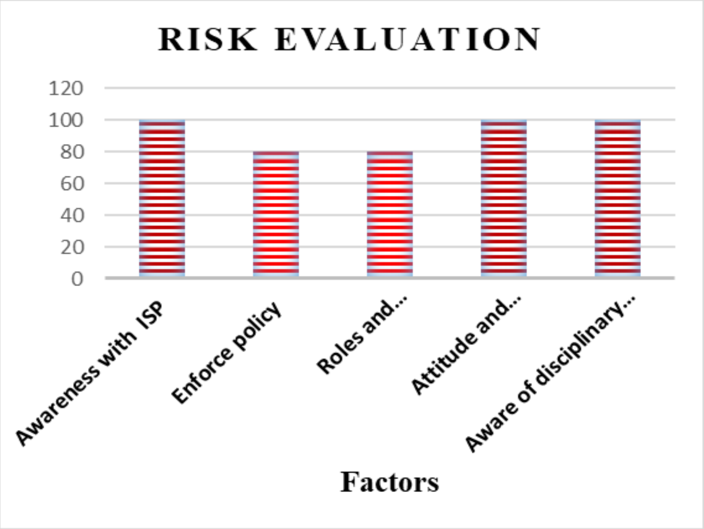

Figure 2: Risk effect on CIA for factors

VI. CONCLUSION

This study focuses on the information security policy of government companies in Libya. The study aims to assess the hypothetical risks of implementing an information security policy, as well as to examine the vulnerabilities and effectiveness of such a policy. The results found that the companies suffer from issues in the implementation of the ISP. It is not enough to have a good ISP without proper implementation. From the viewpoint of threats, having a bad ISP is the same as having a good ISP with bad implementation, as the overall effect is the same. It is strongly recommended that the companies consider a proper implementation of their ISP to benefit from it. The companies are encouraged to focus on the factors identified in the government companies. The study also found that the companies do not have a comprehensive information security policy in place. This is a serious issue, as a comprehensive information security policy is essential for protecting the company's data from unauthorized access. The policy should address several issues, including employee training, security procedures, and the use of security technologies. The study concludes that the implementation of a comprehensive information security policy is essential for protecting government companies from cyberattacks. However, it is important to note that the implementation of an information security policy is only one part of the equation. Companies must also focus on employee training, security procedures, and the use of security technologies to protect their data from unauthorized access. The study focuses on evaluating the information security policy of government companies in Libya. Its primary objectives are to assess the potential risks associated with implementing such a policy and to analyze the vulnerabilities and effectiveness of the policy. The findings indicate that the company faces challenges in implementing its information security policy, highlighting the significance of proper implementation rather than solely possessing a well-designed policy. The study emphasizes that having a poorly implemented policy yields similar consequences as having a well-designed policy with inadequate implementation. To derive maximum benefits from the information security policy, it is strongly recommended that the company prioritize effective implementation. The identified factors specific to the government companies should be given due attention. Additionally, the study reveals that the company lacks a comprehensive information security policy. This is a critical concern since a comprehensive policy is crucial for safeguarding the company's data against unauthorized access. The policy should address various aspects, including employee training, security procedures, and the utilization of security technologies. The study concludes by emphasizing that the implementation of a comprehensive information security policy is vital for protecting government companies from cyberattacks. However, it is important to recognize that policy implementation alone is not sufficient. The companies must also focus on employee training, security procedures, and the deployment of appropriate security technologies to ensure the protection of their data against unauthorized access. In summary, the study recommends an emphasis on the proper implementation of the information security policy, the identification of industry-specific factors, and the development and implementation of a comprehensive policy that addresses employee training, security procedures, and the utilization of security technologies. By addressing these aspects, companies can enhance their information security framework and mitigate the risks associated with cyberattacks.

~~VII.~~ RECOMMENDATIONS

- Government companies should implement a comprehensive information security policy (ISP) that provides clear guidance and direction to all members of the organization regarding the management and protection of information assets. The ISP should be developed using effective processes, including awareness training, compliance monitoring, and regular auditing.
- Government companies should establish a dedicated information security department at the highest possible level within the organization, demonstrating a commitment to making information security a top priority. Sufficient resources should be allocated to ensure the effective operation of the information security function.
- Government companies should design and implement an ongoing awareness training program to familiarize all employees, including managers, with the ISP. Additionally, regular updates on any changes to the ISP should be provided through an established awareness program.
- Government companies should actively encourage greater cooperation and involvement from managers in the implementation and enforcement of the ISP. Managers should be engaged in the process and play an active role in promoting information security practices within their respective areas of responsibility.
- Government companies should foster a culture where employee initiative is valued and encouraged, particularly when it comes to implementing and enforcing the ISP. Managers should actively support and promote employee participation in information security initiatives.
- Government companies should strive to integrate the ISP seamlessly into job processes, minimizing the need for employees to deviate from their regular tasks to follow ISP instructions and practices. This can be achieved through clear communication, training, and the alignment of information security practices with existing job processes.
- Government companies should, Once policies are developed, ensure they are effectively communicated to all employees within the government organization. Use various channels such as official memos, intranet portals, email communications, and training sessions to disseminate policy information. Provide employees with easy access to the policies and any supporting documents.
- Government companies should require employees to acknowledge their understanding of the policies by signing an acknowledgment form or electronically accepting the policies. This formal acknowledgment serves as evidence that employees are aware of the policies and their responsibilities.
- Government companies should establish mechanisms to monitor compliance with policies within the government organization. This can include regular audits, assessments, or reviews to identify any non-compliance or gaps. Utilize technology tools, access logs, and reporting systems to track and monitor adherence to policies.
- Government companies should define clear consequences for policy violations and ensure consistent enforcement across the organization. Consequences can range from verbal warnings and written reprimands to disciplinary actions, depending on the severity and frequency of non-compliance. Ensure that the consequences are communicated to employees in advance

VIII. REFERENCES

[1] Safa, N., Ghani, N. and Ismail, M. 2014. An artificial neural network classification approach for improving the accuracy of customer identification in e-commerce. Malays J Computer Sci, vol 27(3), 171–85.

[2] Ibrahim Al-Mayahi and Sa’ad P. Mansoor. 2013. Information Security Culture Assessment: Case Study. Third International Conference on Information Science and Technology, Yangzhou, Jiangsu, China, 23-25.

[3] Klein, R. H. and Luciano, E. M. 2016. What Influences Information Security Behavior? A Study with Brazilian Users. JISTEM-Journal of Information Systems and Technology Management, vol13 (3), 479-496.

[4] Richardson. R, 2008. CSI computer crime and security survey. Computer Security Institute, http://www.gocsi.com

[5] J. S. Lim, S. Chang, S. Maynard, and A. Ahmad. 2010. Embedding Information Security Culture Emerging Concerns and Challenges. In Proceeding Pacific Asia Conference on Information Systems, PACIS 2010.

[6] Guo, K.H.2013. Security-related behavior in using information systems in the workplace: a review and synthesis. Compute Secure. Vol 32, 242–251.

[7] Alshaikh, M., Maynard, S., Ahmad, A. and Chang, S. 2016. Information Security Policy: A Management Practice Perspective. In Proceeding Australasian

Conference on Information Systems, Adelaide, South Australia.

[8] Ključnikov, A., Mura, L. and Sklenar, D. 2019. Information security management in SMEs: factors of success. Entrepreneurship and Sustainability. Vol 4 (37).2081-2094.

[9] F. Al-Izki and G. R. S. Weir. 2016. Management Attitudes Toward Information Security in Omani Public Sector Organisations. Cybersecurity and Cyberforensics Conference (CCC), Amman, 107-112.

[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] Carvalho, I., Cruz, F. and Almeida, F. 2018. Structure and Challenges of a Security Policy on Small and Medium Enterprises. KSII Transactions on Internet and Information Systems.

[12] Al-Shanfari, Warusia Yassin, Nasser Tabook, Roesnita Ismail, and Anuar Ismail. 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] Alkhurayyif, Yazeed and Weir, George. 2017. Readability as a Basis for Information Security Policy Assessment. Seventh International Conference on Emerging Security Technologies (EST), 114-121.

[14] Rathika Palanisamy, Azah Anir Norman and Miss Laiha Mat Kiah. 2022. Journal of Computer Information Systems, Vol 62 (1), 61-72.