Information Security Policy Implementation Assessment in Libyan Telecommunications Companies

Salima Benqdara
University of Benghazi

Ibrahim Alshiekhy

ABSTRACT

The telecommunications industry is a critical infrastructure that is essential for the functioning of modern society. It is also a lucrative target for cyber attacks. A successful attack on a telecommunications network could potentially expose the information of millions of customers. This study focuses on the information security policy of telecommunications 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 interview technique was selected to collect data and conduct the necessary analysis to verify the existence of any gaps. The study found that several vulnerabilities exist in telecommunications information security policies. It is therefore important for telecommunications companies to take steps to mitigate these vulnerabilities and protect their networks from cyberattacks. Overall, the study provides valuable insights into the importance of information security in the telecommunications industry. The study findings can help telecommunications companies to develop and implement effective information security policies that can help to protect their networks from cyber attacks.

General Terms

Information security policy Implementation.

Keywords

Information security, policy Implementation Assessment, information security management.

1. INTRODUCTION

In recent years telecommunications revolution has made the world as small as ever been any time before. Telecommunications services, like health providers, police departments, and banks. have become vital to the overwhelming majority of people in the world. These services are the backbone of our modern civilization. People, organizations, and even governments all over the world rely heavily on these services either to provide public services or to interchange basic services via the Internet. Any shortage in this service will impose huge losses. Telecommunications organizations also keep a detailed database of their customers. If such a database is exposed to any third party that could impose a huge risk for the user and the service provider. In terms of this, it could be easily understood the importance of the existence of a strong information policy in those organizations specifically [1].

Information security is of major importance to any organization. Information security protects data resources and upholds the three foundations of data security: confidentiality, integrity, and the availability of data. This is partially due to the increasing rate of threats against information technology infrastructure worldwide. Information security issues persist in organizations in light of continued data breaches, systems outages, and malicious software [2]. Information security policy provides the necessary platform and environment of regulations in an organization to control users' security-related behavior [3]. Policies direct how issues should be addressed and technologies should be used. Policies do not specify the proper operation of equipment or software—this information should be placed in the standards, procedures, and practices of users' manuals and systems documentation. It must be clear that Policy should never contradict the law because this can create significant liability for the organization. Security policies are the least expensive control to execute, but the most difficult to implement properly [2].

Threats by their nature; originate from various sources including policy issues, policy implementation issues, and/or employees' security-related behavior. human aspects of information security remain a critical and challenging component for creating a safe and secure information environment [3]. Also, A survey conducted by the Computer Security Institute reported that the average monetary loss per incident was $288,618 and that 44% of those who responded to the survey reported insider security-related abuse, making it the second-most frequently occurring computer security incident [4]. In the absence of a strong, properly formulated Information security policy, the anticipated security-related behavior of employees would be much more difficult to control or punish. The expected severity of such a situation is catastrophic to any organization; taking into consideration that up to 80% of major security breaches in an organization result from the incorrect behavior of employees, rather than from any technical weakness in the information systems of the organization [5]. the information systems (IS) security literature highlights and exhibits a growing interest in investigating the issue of employee behavior that may have security implications in organizations [6]. In line with this, similar growth in policy adoption in firms and organizations should take place to mitigate the consequences of such mentioned behavior.

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

Alshaikh et al., (2016) developed a model of information security policy management practice. The model consists of three institutionalization stages: the development stage, the implementation and maintenance stage, and the evaluation stage. Each stage consists of several practices containing management activities. The study highlights the relationship between Information Security Policy and managerial practices in organizations. The result findings several drawbacks that reduce the ability of organizations regarding managerial practices in implementing a security policy.

Ključnikov et al., (2019) Identify the factors for the success of information security management in the segment of SMEs in Slovakia. The results show that Security Controls, like the application of standards, technical and procedural information security controls, and risk management reflect the success of information security management. The second most important factor is the supportive top management. The results indicate that SMEs should promote organizational awareness in information security management in line with the implementation of security controls as the first line of defense to protect the information, as the most valuable asset of the company.

Al-Izki and Weir (2016) Presented a study to measure management attitudes toward Information Security in Oman. The study considers how such attitudes influence Information Security governance. In addressing these issues, review current compliance with Information Security procedures in Omani public sector organizations; review management attitudes toward Information Security governance practices; and explore how management attitudes toward Information Security affect these aspects. The results showed a considerable lack of management interest in Information Security in Omani public sector organizations. In addition, results revealed a strong relationship between management attitude toward Information Security and aspects indicating the management governance activities. The study concluded that there is a strong relationship between management attitude toward Information Security and compliance with Information Security policies.

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.

Carvalho et al., (2018) proposed a study to identify the most important and the least relevant elements in the structure of a security policy. It presents a synthesis of the literature on information security policies content and it characterizes 15 Small and Medium Sized Enterprises (SMEs). The content analysis (CA) research technique was applied to characterize the information security policies. The study shows that the relative importance of these elements is slightly changed according to the sectors of activity. SMEs need to be aware of these elements to design their security policies in a precise, concise, and unambiguous way.

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.

Alkhurayyif et al., (2017) present study investigates the effectiveness of applying readability metrics as an indicator of policy comprehensibility. The paper focused on assessing the readability factor in affecting the success or effective operation of ISPs.Results from a preliminary study reveal variations in the comprehension test results attributable to the difficulty of the examined policies. The result shows some correlation between the software readability and human comprehension test results and supports our view that readability has an impact on understanding ISPs. These findings have important implications for users' compliance with information security policies and suggest that the application of suitably selected readability metrics may allow policy designers to evaluate their draft policies for ease of comprehension before policy release. Indeed, there may be grounds for a readability compliance test that future ISPs must satisfy.

Rathika et al., (2022) Introduce a study to review, the literature to gather evidence related to the risk of non-compliance to the security policy for employee behavior. The purpose of the study gathers evidence related to the risk of non-compliance to the security policy for employee behavior and mitigation strategies to address them. The risks are mapped according to the People, Process, and Technology (PPT) Model. The review finds that security policy compliance in a BYOD environment is still sporadic.

3. PROPOSED APPROACH

A telecommunication company was chosen to be the case study of this research. The ISP of this particular company was investigated and proved to be optimum, updated, and well-compliant with international information standards. On the other hand, it was revealed the existence some issues in the implementation of the ISP. The implementation process in that company was investigated using Interview Method. Taking into account that the implementation process is the responsibility of the managerial level in the company. The process of the proposed approach is as follows:

- Data Collected: A qualitative research method was followed by interviewing the manager level in the company to collect data on the current security. the interview has been carefully designed to clarify the managerial aspects of ISP implementation. It was also designed to give the interviewed personnel enough space and freedom to express any thoughts or ideas he/she got toward the subject. questions of the interview are prepared in advance, they are mapped to seven categories of data as shown in Table 1.

Table 1: Mapping interview questions to interview aspects

Factor No.	Category	Question	Highlight
1	ISP Awareness	Q1	• awareness with ISP in the organization
2	Enforce policy in the organization	Q2	• enforce policy in the organization
3	Roles and Responsibilities	Q3	• roles and responsibilities in general regarding the ISP in the organization
4	Employee attitude of compliance with the ISP	Q4	• Attitude and point of view toward compliance with the ISP
5	compliance with the ISP	, Q5	• compliance with information security policy
6	Policy breach penalties	Q6	• Aware of disciplinary penalties for noncompliant behavior with the information security policy in the organization y

- Data Analysis: After data and information are collected risk assessment analysis is used to analyze those collected data. Evaluating the current status of the security strategy by interviewing the company's managers and analyzing the current situation by identifying the security gaps. in this study, a risk matrix is used as a risk assessment technique to define the level of risk by considering the aspect's severity against the aspect's probability or likelihood as suggested by Mr. Mohan Kamat in his contribution to the (ISO 27001 Implementer’s Forum) that took place in 2009 [6]. This is a simple mechanism to increase the visibility of risks and assist management decision-making. The figure below illustrates the utilized risk matrix.

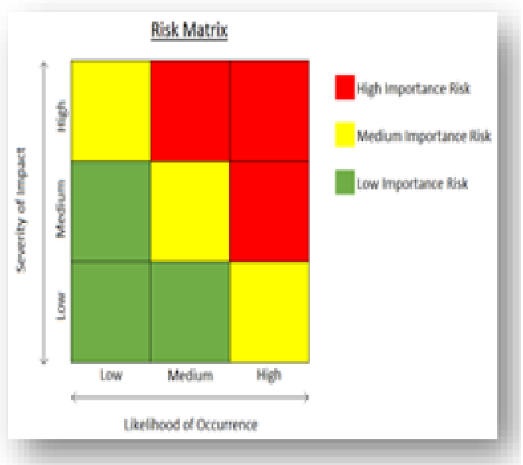


Fig. 1 Risk matrix

4. EXPERIMENTAL SETUP

This section describes the experimental setup which contains two parts

- •Analyzing the current situation by identifying the security gaps based on the data analyzed.
- •In this study, a risk matrix is used during risk assessment to define the level of risk by considering the category of probability or likelihood against the category of consequence severity.

5. RESULTS AND DISCUSSION

5.1 Factor 1

Figure 2 presents a summary of the knowledge of the entity's ISP, and their awareness of its aspects used by the company. The result shows that employees have low knowledge of the entity's ISP and that managers are not aware of ISP details and updates. This is resulting in a high risk to the confidentiality, integrity, and availability of the company's information. The policy is also unrealistic, which decreases its impact and the security standard in the organization. This can lead to cyber-attacks. The absence of an awareness program and lack of implementation of the information security policy has contributed to the shortage of identifying information security risks and the selection of acceptable standards for the company. 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. Thus, a company should implement a security awareness program to improve understanding and awareness of the security policy. The findings of Figure 2 suggest that the company needs to take steps to improve its security posture. Employees have low knowledge of the entity's ISP, and managers are not aware of ISP details and updates. This means that employees may not be taking the necessary steps to protect the company's information, and managers may not be aware of the latest security threats and vulnerabilities. The policy is also unrealistic, which decreases its impact and the security standard in the organization. This can lead to cyber-attacks. The absence of an awareness program and lack of implementation of the information security policy has contributed to the shortage of identifying information security risks and the selection of acceptable standards for the company. 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. The company needs to raise awareness of the security policy, and it needs to invest in tools and resources that will help it to identify and assess security risks. By taking these steps, the company can reduce the risk of cyber-attacks and protect its information.

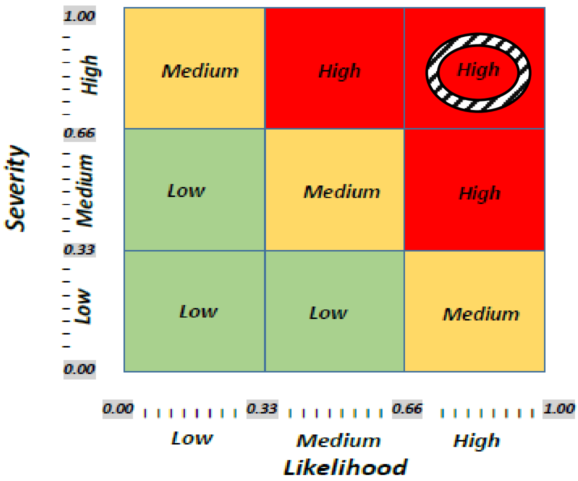


Fig 2: Risk effect on CIA for Information Security Policy Awareness

5.2 . Factor 2

Figure 3 presents a summary of the enforcement policy in the company. The Figure showed that the company has a high risk of confidentiality and integrity breaches. This is due to many factors, including the lack of an enforcement policy, the lack of security experience in the company, and the lack of training for employees on information security. The lack of an enforcement policy means that there is no clear plan for how to respond to security incidents or how mitigate risks. This can lead to delays in responding to incidents, which can make them more difficult to contain. In addition, the lack of an enforcement policy can make it difficult to hold employees accountable for security breaches. The lack of security experience in the company means that there is no one with the necessary skills and knowledge to develop and implement a security program. This can lead to security vulnerabilities that are not identified or addressed. In addition, the lack of security experience can make it difficult to respond to security incidents effectively. The lack of training for employees on information security means that employees are not aware of the risks that they face and the steps that they can take to protect the company's information. This can lead to employees making mistakes that could compromise the company's security. The findings of result suggest that the company needs to take steps to improve its security posture. Employees have low knowledge of the entity's ISP, and managers are not aware of ISP details and updates. This means that employees may not be taking the necessary steps to protect the company's information, and managers may not be aware of the latest security threats and vulnerabilities. The policy is also unrealistic, which decreases its impact and the security standard in the organization. This can lead to cyber-attacks. The absence of an awareness program and lack of implementation of the information security policy has contributed to the shortage of identifying information security risks and the selection of acceptable standards for the company. 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. the company can reduce the risk of security breaches and protect its information by implementing a security awareness program to improve understanding and awareness of the security policy.

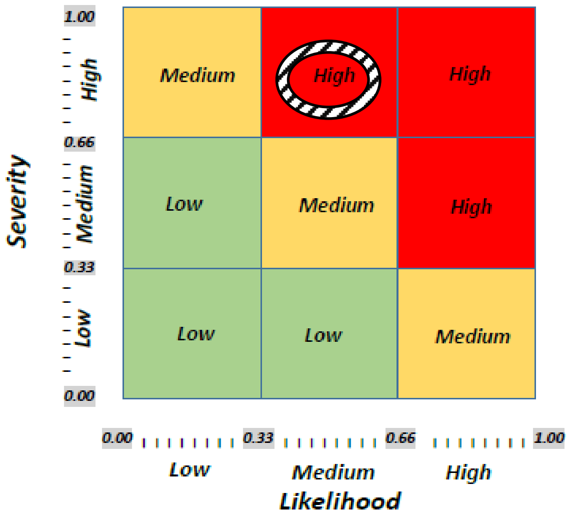


Fig 3: Risk effect on CIA for enforcing policy in the company

5.3 Factor 3

Figure 4 presents a summary of the roles and responsibilities in general regarding the ISP in their departments and among their employees. The figure shows that the risk effect on confidentiality and integrity is high. The results show that the management team's role in information security planning (ISP) is minor and passive. This means that the management team is not actively involved in setting or enforcing the ISP. This is a serious issue, as the management team is ultimately responsible for the security of the company's information. The results indicated that the management role is minor and passive toward ISP tasks. In some rare situations, the managers are addressed directly with some instructions. This is partially caused by a lack of knowledge, specialization, and job description. This means that the management team does not have the necessary knowledge or experience to set or enforce the ISP. In addition, the management team's job description does not include any specific responsibilities for information security. The result concluded that a lack of segregation of 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 vectors. This means that the company does not have a system in place to separate different duties and responsibilities.

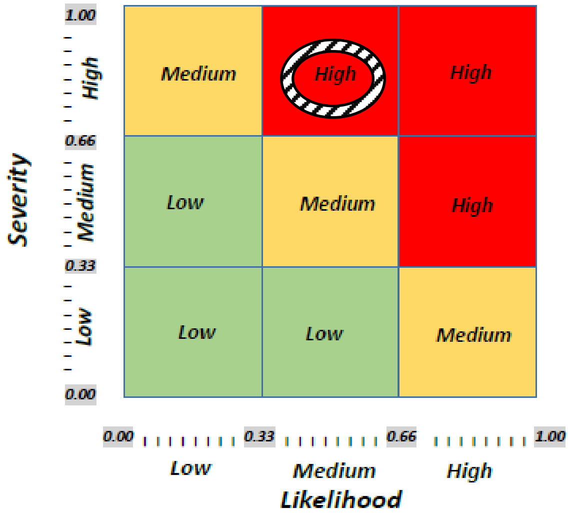
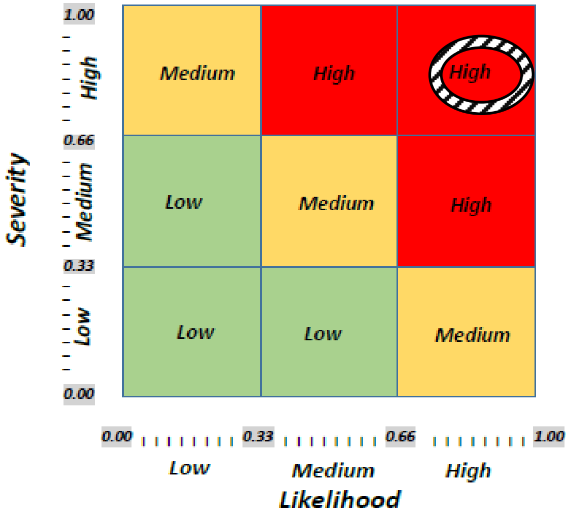


Fig 4: Risk effect on CIA for roles and responsibilities in the ISP

5.4 Factor 4

Figure 5 illustrates the attitude and point of view toward compliance with the ISP in the company. The results show that the risk effect on confidentiality, integrity, and availability is high. The results find that managers do not have any intentions to be incompliant with ISP in normal situations. They only tend to do so as an exception if there is no way else to carry out their job. One of the managers noted that when he was on a vacation outside Libya, and he could not access his job's account remotely via VPN, he had no choice but to call a colleague and give him his access credentials such as username and password to accomplish the task locally. He admits that his behavior is illegal and insecure, but he says it was the only way to accomplish the urgent task. Such behavior is very unprofessional and irresponsible. Which identifies the organization to become the target of social engineering attacks. The management team's lack of involvement in setting and enforcing the ISP is a serious issue because it means that the management team is not taking the security of the company's information seriously. The management team is ultimately responsible for the security of the company's information, and they need to be actively involved in setting and enforcing the ISP to protect the company from security breaches. Moreover, the lack of segregation of duties poses the risk that employees will be able to access, alter, or destroy information that they should not be able to access, alter, or destroy. This risk is increased when employees have access to multiple systems and data sets, as they may be able to use this access to commit fraud or other unauthorized activities. For example, an employee who has access to both the company's financial records and its customer database could potentially steal money from the company by making fraudulent entries in the financial records and then using the customer database to identify customers who are likely to be targeted for fraud. To mitigate this risk, organizations should implement segregation of duties controls that ensure that no one employee has access to all of the information and systems that they would need to commit fraud or other unauthorized activities. This can be done by assigning different employees to different tasks and by implementing access controls that restrict employees' access to information and systems. Segregation of duties is an important control that can help to protect organizations from fraud, errors, and other security risks. By implementing segregation of duties controls, organizations can help to ensure that their information is secure and that their processes are efficient and effective. In addition, the company should consider hiring a qualified security professional to help them develop and implement an information security program. A security professional is an individual who has the knowledge and skills to assess and mitigate security risks. They can help the company identify its security risks, develop appropriate controls to mitigate those risks and train employees on how to protect the company's information. The company should also consider conducting regular security audits to identify any vulnerabilities in its information security program. A security audit is a process of reviewing a company's information security controls to identify any weaknesses that could be exploited by attackers. By conducting regular security audits, the company can identify and fix any vulnerabilities in its information security program before they can be exploited.



.**Fig 5: Risk effect on CIA for employee attitude of compliance with the ISP**

5.5 Factor 5

Figure 6 shows the company's compliance with the ISP. The company has a medium level of compliance, which means that they are generally following the ISP's rules, but there are some areas where it could improve. The company is doing well in some areas, such as having a clear and concise policy on ISP compliance. They also have a good system in place for monitoring and reporting on compliance. However, there are some areas where the company could improve. For example, they could provide more training to employees on ISP compliance, and they could also conduct more regular audits of compliance. The results indicate that the company has limited experience in enforcing ISP rules. This could be due to some factors, such as the company being relatively new or the ISP's rules being complex. However, the company needs to develop a strong enforcement policy to ensure compliance with the ISP's rules. The results also indicate that the company has not encountered any difficulties with compliance in the past. This is positive, as it suggests that the company is generally following the ISP's rules. However, it is important to note that the company may not have encountered any difficulties yet, but this does not mean that it will not in the future. The company needs to continue to monitor compliance and take steps to address any issues that arise. The results conclude that the company is willing to comply with the ISP's policy. This is positive, as it suggests that the company is committed to following the ISP's rules. However, it is important to note that willingness to comply is not the same as actually complying. The company needs to take steps to ensure that its employees are following the ISP's rules. The results also conclude that the company lacks enforcement and inconsistent auditing of the policy. This means that the company is not doing enough to ensure that its employees are following the ISP's rules. The company needs to develop a strong enforcement policy and implement regular audits to ensure that its employees are complying with the ISP's rules. The lack of enforcement and inconsistent auditing can have several negative impacts on the company. First, it can lead to security breaches. If employees are not following the ISP's rules, they may be more likely to accidentally or intentionally expose the company to security threats. Second, it can lead to fines and penalties from the ISP. If the ISP finds that the company is not complying with its rules, it may impose fines or penalties on the company. Third, it can damage the company's reputation. If customers find out that the company is not following the ISP's rules, they may be less likely to do business with the company. The company should develop a strong enforcement policy, implement regular audits, provide training to employees, and monitor compliance on an ongoing basis. By Providing awareness and training to employees, the company can improve its compliance with the ISP's rules and reduce the risk of security breaches, fines, and reputational damage.

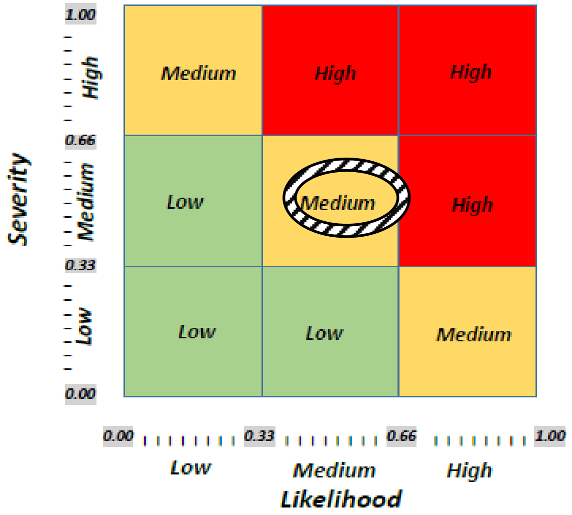


Fig 6: Risk effect on CIA for compliance with the ISP

5.6 Factor 6

Figure 7 presents a summary of the Aware of disciplinary penalties for noncompliant behavior with the information security policy in the company. The figure shows that the risk effect on effects on confidentiality, integrity, and availability is high. The result shows that employees are aware of the potential risks of non-compliance with the information security policy, but they are not aware of the specific disciplinary penalties that may be imposed for non-compliance. This lack of awareness could lead to irresponsible behavior, as employees may not believe that there are any serious consequences for non-compliance. The results also show that there have been some isolated cases of disciplinary penalties being imposed for non-compliance, but these cases have been rare. This suggests that the company may not be taking information security seriously enough and that employees may not believe that there is a real risk of being punished for non-compliance. The lack of awareness of the importance of the security policy and the lack of consequences for non-compliance can create several problems for the company. First, it can lead to employees being more likely to engage in risky behavior, as they do not believe that there are any serious consequences for doing so. Second, it can make it more difficult for the company to enforce the security policy, as employees may not believe that they need to comply with it. Third, it can make it more difficult for the company to respond to security incidents, as employees may not be aware of the risks involved or the steps that they need to take to protect the company's data. To address the problems identified in Figure 7, the company should increase awareness of the importance of the security policy, enforce the security policy consistently, and create a culture of security. the company can create a culture where employees are aware of the importance of security and are committed to protecting the company's data.

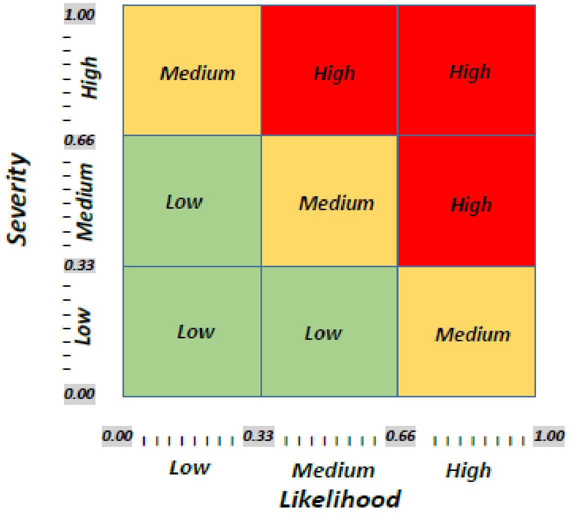


Fig 7: Risk effect on CIA for Policy breach penalties

5.7 Comparison of the risk effect on the factors

Table 2 and Figure 8 illustrate the estimated risk effect of every element on the three elements of the CIA triad. The results show that the telecommunication company has a high risk of security breaches in the areas of confidentiality, integrity, and availability. This means that there is a high risk that information may be disclosed to unauthorized individuals, modified without authorization, or not available when needed. The results find that the company suffers from issues in the implementation of the ISP. This led to a lack of enforcement and inconsistency auditing of the policy. The impact will affect the security standard overall and initiate chaos in the organization, which can lead to cyber-attack. The results concluded that the company considers a proper implementation of its ISP to benefit properly from it. The company is encouraged to concentrate on the factors identified in the telecommunication company. To address the problems identified in Figure 7, the company should increase awareness of the importance of the security policy, enforce the security policy consistently, and create a culture of security. The results of the study suggest that the telecommunication company needs to take steps to improve its information security posture. The company should implement strong security controls, such as encryption, access control, and intrusion detection. The company should also train its employees on security best practices and should conduct regular security audits. By taking these steps, the company can reduce its risk of security breaches and protect its data.

6. CONCLUSION

This study focuses on the information security policy of telecommunications 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 company suffers 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 company consider a proper implementation of its ISP to benefit from it. The company is encouraged to focus on the factors identified in the telecommunications company. The study also found that the company does 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 telecommunications companies from cyberattacks. However, it is important to note that the implementation of an information security policy is only one part of the equation. The company must also focus on employee training, security procedures, and the use of security technologies to protect its data from unauthorized access.

7. RECOMMENDATIONS

- The organization should implement an information security policy (ISP) that provides guidance and direction to all members of the organization regarding the management and protection of information assets. The ISP should be implemented using effective processes that include awareness training, compliance monitoring, and auditing.
- The organization should establish an information security department at the highest possible level in the organization and make information security a priority. The organization should commit enough resources for the operation of information security.
- The organization should establish an awareness training program to introduce its ISP to all employees, including managers. The organization should also establish an awareness program to update employees on changes to the ISP.
- The organization should encourage more cooperation and involvement from managers in the process of implementing and enforcing the ISP.
- The organization should make employee initiative a part of the culture of managers for implementing and enforcing the ISP.
- The organization should simplify the integration of the ISP with job processes to avoid having to turn around ISP instructions and practices.

8. 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.

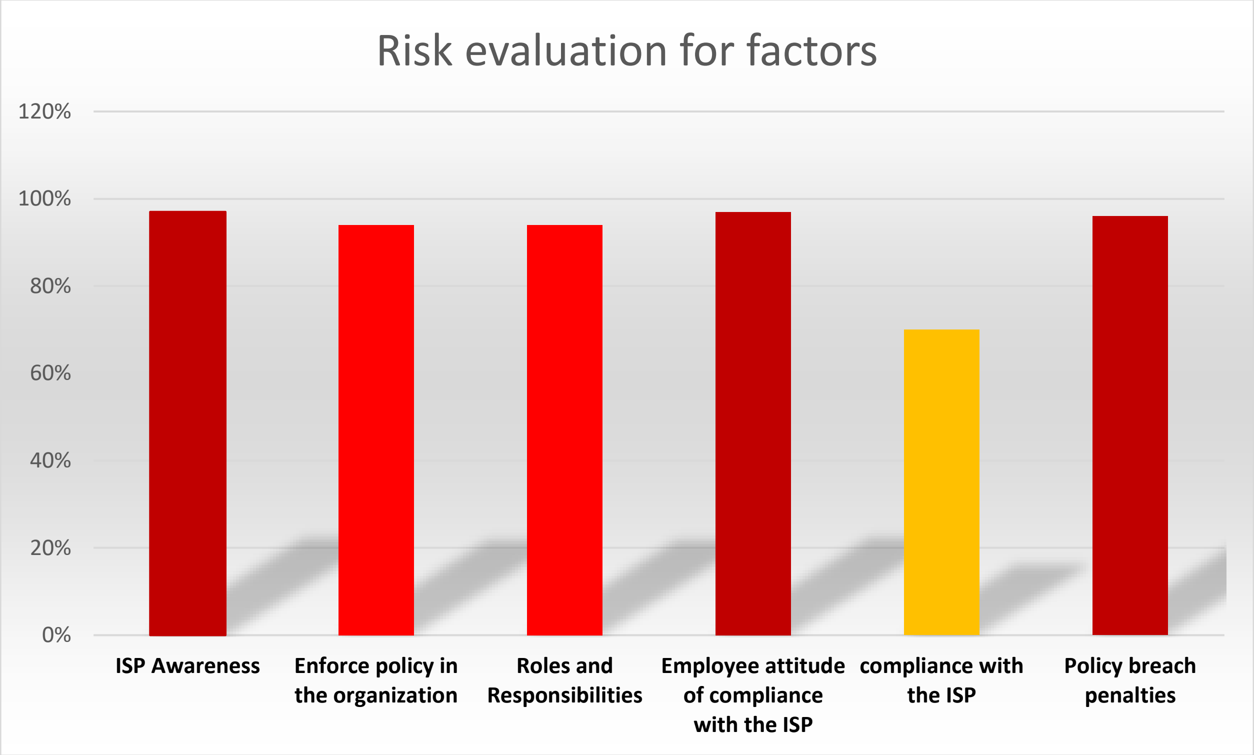


Fig 8: Risk effect on CIA for factors

Table 2: Mapping estimated risk effect of every factor on the three elements of the CIA

Factor No.	Highlight	Effect			Risk evaluation	Consequences
		C	I	A		
1	• awareness with ISP in the organization	✓	✓	✓	High	• Overall negative effects on confidentiality, integrity, and availability • The policy will be impractical which will decrease the impact of the policy and the security standard in the organization. That will lead to a cyber attack
2	• Enforce policy in the organization	✓	✓		High	• 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.
3	• Roles and Responsibilities in general regarding the ISP in the organization	✓	✓		High	• Negative effects on confidentiality and integrity • 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 vector
4	• Attitude and point of view toward compliance with the ISP	✓	✓	✓	High	• Overall negative effects on confidentiality, integrity, and availability • Such behavior is very unprofessional and irresponsible. Which identifies the organization to become the target of social engineer attacks.
5	• Compliance with information security policy	✓	✓		Medium	• Negative effects on confidentiality and integrity • According to the interview answers, that indicates the willingness to comply with the

						policy however, the lack of enforcement and inconsistency auditing on the policy. The impact will affect the security standard overall and initiate chaos in the organization which can lead to cyber-attack.
6	• Aware of disciplinary penalties for noncompliant behavior with the information security policy in the organization	✓	✓	✓	High	• Overall negative effects on confidentiality, integrity, and availability • The lack of awareness of the importance of the security policy in the organization can lead to irresponsible behavior that put the organization as a target for threat vectors. also, lack of consequences or pantiles in the organization creates disciplinary issues which will impact vulnerability severity in the organization's