International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Assessing Cybersecurity Threats and Awareness in Bosaso's Banking and Telecom Sectors

Mohamed Abdirisak Buraale[1], Dr. Tiktik Khawa Abdurrahman[2], Dr. Fazilah Che Fauzi[3]

[1]Asia e University Malaysia
Email: *mohamedqalinmaal[at]gmail.com*

[2]Principle Supervisor, Professor, Asia e University
Email: *titik.khawa[at]aeu.edu.my*

[3]Program Coordinator and Professor, Asia e University
Email: *fazilah.chefauzi[at]aeu.edu.my*
Orcid: https://orcid.org/0009-0002-3146-6818

Abstract: ***Cybersecurity is a critical concern for the banking and telecom sectors, which are prime targets forcyber threats. In Bosaso, Somalia, the increase digital technologies has outpaced the implementation of effective cybersecurity measures. This study aims to evaluate the current levelof cybersecurity awareness among IT professionals in Bosaso's banking and telecom sectors and to identify key vulnerabilities and threats confronting these industries. A quantitative survey was conducted, targeting IT professionals in Bosaso's banking and telecomsectors. The survey assessed participants' awareness of cybersecurity threats, their confidence in existing security measures, and their experiences with cyber incidents. Data were analyzed using descriptive statistics and thematic analysis to elucidate common themes and patterns. The survey revealed that while the majority of IT professionals are aware of common cybersecurity threats, there is a significant lack of confidence in the adequacy of current security measures. Key vulnerabilities identified include inadequate employee training, outdated software, and insufficientinvestment in advanced security technologies. Furthermore, 65% of respondents reported experiencing at least one cyber incident in the past year. These findings underscore the urgent needfor enhanced cybersecurity practices. The study highlights the critical need for improved cybersecurity training programs, substantial investment in modern security technologies, and the implementation of comprehensive cybersecurity policies in Bosaso's banking and telecom sectors.Addressing these issues is essential for safeguarding sensitive information and ensuring the resilience of these critical infrastructure***

Keywords: Cybersecurity, Bosaso, Private Sectors, Security Challenges, Threats, Awareness, IT Professionals, Data Protection, Vulnerabilities, Digital Security, Risk Management, Information Security

1. Introduction

The rapid adoption of digital technologies in Bosaso, Somalia, has significantly outpaced the implementation of effective cybersecurity measures, thereby elevating significant risks in the banking and telecom sectors. Cybersecurity remains a critical concern for these sectors as theyare prime targets for cyber threats. Despite advancements in information and communication technology (ICT) that have transformed organizational approaches to business strategy and management, there is a noticeable gap in cybersecurity practices. This study addresses the pressing issue of inadequate cybersecurity awareness and practices among IT professionals in Bosaso's banking and telecom sectors. The primary problem is the insufficient implementationof robust cybersecurity measures, which leads to increased vulnerability to cyber threats. Thesignificance of this study lies in its potential to enhance the cybersecurity posture of critical sectors in Bosaso. By identifying key vulnerabilities and assessing the level of awareness, the research provides actionable insights that can inform policy and strategic decisions. Improvingcybersecurity practices is crucial for safeguarding sensitive information and ensuring the operational resilience of these sectors. The main aim of this paper is to assess cybersecurity threats and awareness in Bosaso's banking and telecom sectors, identify key vulnerabilities andthreats confronting these industries, and provide recommendations for improving cybersecurity measures and policies. Previous studies have highlighted various cybersecurity threats, such as spam attacks, malware, phishing, and DDoS attacks, which pose significant risks to data integrity and security (Kaspersky Lab, 2015; Rouse, 2019). Despite the global emphasis on cybersecurity, there is limited research focusing specifically on the unique challenges faced by developing regions like Bosaso, Somalia. The literature lacks comprehensive studies on the cybersecurity awareness and practices within Bosaso's banking and telecom sectors, thereby presenting a critical research gap that this study aims to fill. Organizations worldwide prioritize cybersecurity, with over 50 countries developing policies to combat cybercrimes (CISA, 2023). However, the situation in Somalia, particularly in urban centers like Bosaso, remains under-researched. Existing literature emphasizes the need for secure network infrastructures and comprehensive security measures (Cisco, 2020; Tonggal, 2020). Despite these global advancements, Somalia's cybersecurity infrastructure lags, exposing critical sectors to severe risks (Gagliardone & Sambuli, 2015). Cybercrimes, including digital fraud, identity theft, cyber espionage, and ransomware attacks, have substantial financial and operational impacts on businesses and economies (Symantec, 2020; McAfee, 2020).

2. Methodology

The study employed a quantitative research methodology to Cybersecurity Challenges and Awareness in Bosaso's Private Sectors Bosaso. This approach facilitated the use of statistical analysis to generalize findings across a broader population, thereby providing a quantitative basis for understanding

cybersecuritypractices within the targeted demographic. The Survey Monkey platform was selected for its ease of use and cost-effectiveness, allowing for efficient data collection and analysis. The online questionnaires were divided into two parts, focusing on different sectors: banking institutions and telecom institutions. This targeted approach helped in collecting relevant data specific to the industries involved. The study aimed tomeasure both independent and dependent variables related to cyber security awareness. Independent variables included factors like data interception and identity theft, while the dependent variable was the level of cyber security awareness among participants. The survey consisted of 15 items, utilizing a Likert scale (1 to 5) for responses. This scale allowed participants to express their level of agreement or awareness regarding various cyber security issues, facilitating the measurement of attitudes and knowledge. A simplerandom sampling method was used to distribute the surveys via email to specific organizations, ensuring that the sample was representative of the target population. This method helped in achieving a valid response rate.

3. Research Design

Table 3.1: Questionnaire Design

Section	Variable	Scale of Measure
Section A: Demographic Profile	Gender	Nominal
	Age	Nominal
	Job Type	Nominal
Section B: Cybersecurity Awareness Level	Cybersecurity Awareness Level	Likert Scale (5- point)
	Factors Influencing Cybersecurity Awareness	Likert Scale (5- point)
	Current Countermeasures and Strategies	Likert Scale (5- point)
1. Cybersecurity Awareness Level	1.1: Rate your confidence in cybersecurity awareness from 1 to 5, where 5 indicates extremely confident and 1indicates not at all confident.	Likert Scale (5-point)
	1.2: Use of antivirus solutions	Likert Scale (5-point)
	1.3: Access control lists	Likert Scale (5-point)
	1.4: Overall awareness level of cybersecurity	Likert Scale (5-point)
2. Countermeasures andStrategies	2.1: Level of security measures implemented in the private sector banks in Bosaso to segregate differenttypes of information (e.g., financial, legal, HR) and manage access.	Likert Scale (5-point)
	2.2: Security measures for connecting external devicesto office computers	Likert Scale (5-point)
	2.3: Inclusion of drafted policies, plans, and guidelineswithin the cybersecurity program	Likert Scale (5-point)
	2.4: Information security awareness training conductedby the company within the past 12 months	Likert Scale (5-point)
3. Factors Influencing Cybersecurity Awareness	3.1: Occurrence of cyber-attacks against your bank inthe last 12 months	Likert Scale (5-point)
	3.2: Significant customer security incidents over the pasttwo years	Likert Scale (5-point)
	3.3: Collaboration with third parties, such as IT serviceproviders, who have access to your information	Likert Scale (5-point)
	3.4: Additional security requirements for third parties, ifapplicable (only if the previous question is answered "Yes")	Likert Scale (5-point)

4. Data analysis and findings

In this study, data were collected using questionnaires that were developed and administered through Survey Monkey. This approach facilitated the acquisition of quantitative data from participants within theprivate sector in Bosaso, Somalia. Following data collection, the information was input into IBM SPSS® software for subsequent analysis. IBM SPSS® is a crucial tool for the management and analysis of statistical data, offering a robust platform for performing a variety of statistical tests and analyses. The analytical process commenced with descriptive statistics, which provided a summary of respondent characteristics. This involved calculating measures such as means and frequencies, and generating graphicalrepresentations of the data. Descriptive statistics play a vital role in distilling extensive data sets into coherent formats, thereby enhancing the identification of trends and patterns.

The below figure 1 presents a breakdown of responses by gender, illustrating a notable imbalance.Out of a total of 55 responses, 31% were from females, equating to 17 responses, while 69% werefrom males, amounting to 38 responses. This disparity suggests that males contributed a considerably larger share of the responses compared to females. Such an imbalance in gender representation can have significant implications. In contexts where balanced input from different genders is crucial, this skewed distribution might lead to a partial or distorted understanding of the subject being examined. For instance, if the responses are related to opinions on a specific issue, the predominance of male responses could result in a viewpoint that does not fully reflect the experiences or opinions of females.

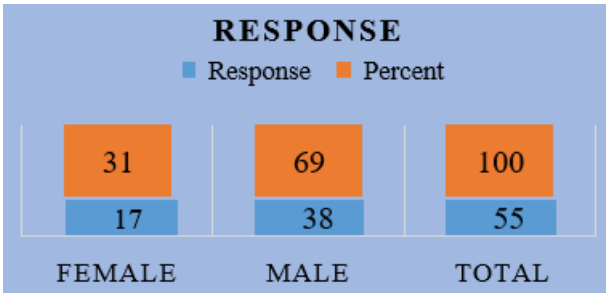

Figure 1: Response Rate

Figure 2 reflecting the degree of confidence in cyber security within telecom and banks in Bosaso, Somalia, presents a concerning picture. Only 7.1% of the respondents expressed

full confidence in their cyber security posture, which is alarmingly low for an industry that handles sensitive financial information. This lack of confidence could have significant implications for the overall security environment in Bosaso's private sector. A notable 46.4% of participants reported only moderate confidence in their banks' cyber security measures. This significant percentage indicatesthat while there is some level of assurance, it is not robust enough to instill full trust among customers. This moderate confidence might stem from partial implementation of security measuresor a lack of visible commitment to cyber security best practices. The most alarming finding is that28.6% of respondents indicated no confidence at all in their banks' cyber security. This high level of insecurity suggests that a substantial portion of the population perceives their financial institutions as vulnerable to cyber threats. This perception could be due to past security incidents,lack of transparency in cyber security practices, or inadequate customer communication regarding security measures. Interestingly, 10.7% of respondents are fairly confident, and another 7.1% areonly moderately confident. These figures, though not large, highlight a segment of the population that recognizes some efforts towards cyber security but still has reservations. This group may require more targeted communication and reassurance about the measures being taken to protect their information. The overall findings indicate that many respondents are unsure whether they can trust their banks' cyber security procedures. This uncertainty points to potential gaps in cyber security awareness and controls within Bosaso's private sector. The lack of confidence among customers could lead to reduced trust in financial institutions, potentially impacting their reputation and customer loyalty.

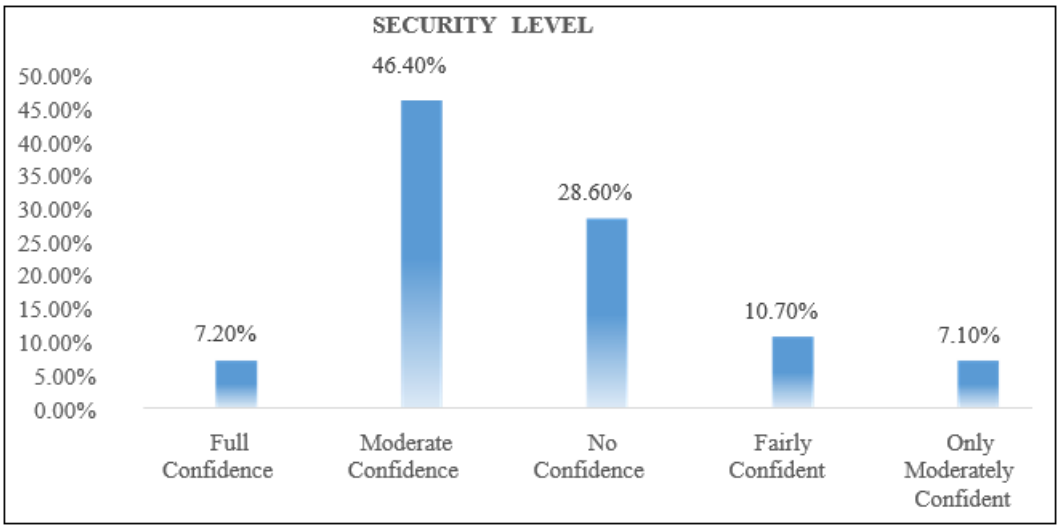

Figure 2: Cybersecurity level Banks and Telecom in Bosaso

Figure 3 provides a detailed examination of access control implementation in Bosaso telecom andbanking institutions, offering significant insights into the current state of data security practices within these organizations. The data reveals a critical need for enhanced access control measures to bolster data protection. Other hand 46.00% of respondents reported that access control is not enabled on their computers. This lack of access control is particularly concerning given the sensitive nature of financial data managed by banks. The absence of such fundamental security measures allows unauthorized individuals to potentially access critical information, posing substantial risks to data integrity and confidentiality. This statistic highlights a significant deficiency in the foundational security infrastructure of many banks in Bosaso. Further complicating the security landscape, 40% of respondents acknowledged having access control mechanisms in place, yet they noted that these controls could be bypassed by workers. This indicates that while some attempts are made to implement security measures, they fall short in effectiveness, leaving room for potential exploitation by both malicious insiders and external attackers. The ease with which these controls can be circumvented underscores the need for stricterenforcement and a thorough reassessment of current access control policies to ensure their robustness and reliability. Unfortunately, only 14.00% of respondents reported that access controlwas not only enabled but also properly managed within their organizations. This low percentage reflects a broader struggle among Bosaso telecom and banks to achieve and maintain effective access control measures. Properly managed access control is crucial for protecting sensitive data by ensuring that access is restricted to authorized personnel only. The limited success in this area highlights the ongoing challenges faced by banks in Bosaso in establishing and enforcing rigorousaccess control practices. In conclusion, the survey results highlights an urgent need for Bosaso telecom and banking institutions to strengthen their data security measures, with a particular emphasis on improving access control protocols.

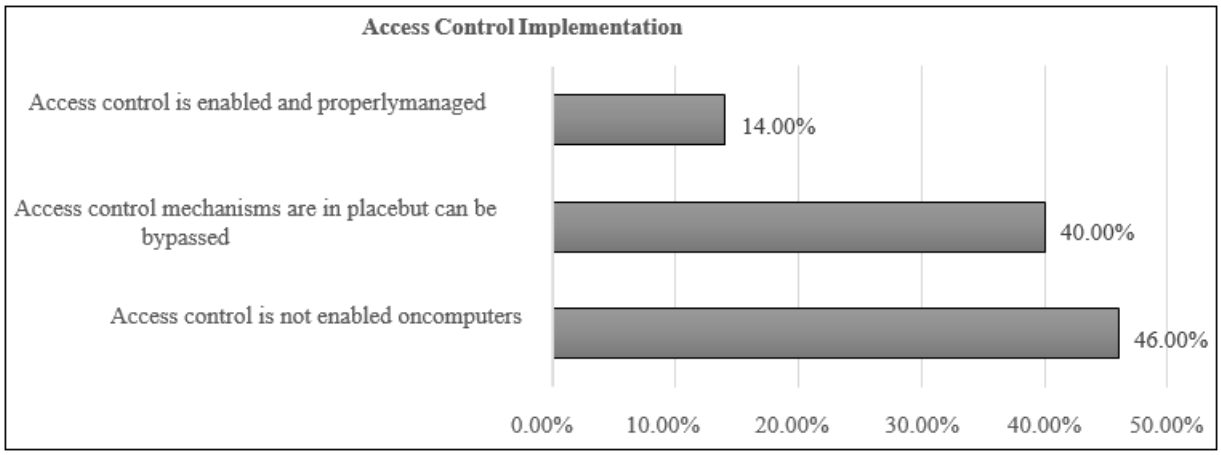

Figure 3: Access Control Implementation

Figure 4 illustrates that 25% of organizations categorize their resources such as data or systems bytype, yet do not delineate specific access permissions for these resources. This approach implies adeficiency in detailed access control mechanisms, potentially exposing sensitive resources to security vulnerabilities due to inadequate protection measures. In contrast, 21.4% of organizationsnot only classify data by type but also assign unique permissions to it. This practice reflects a moresecure data management strategy, ensuring that access is restricted to authorized individuals or roles based on the data type. Despite its advantages, this approach is less commonly adopted compared to the broader practice of resource classification without specific permission assignments. Furthermore, 14.3% of organizations adopt a policy of granting access permissions indiscriminately, permitting access to resources without regard to the individual's role or necessity.Such a practice poses significant security risks, as it fails to limit access based on the principle of least privilege and the sensitivity of the information. Additionally, a notable 39.3% of organizations lack formal information security management policies. The absence of such policies can result in inconsistent data handling and increased security risks, as there are no established guidelines or standards governing the management and protection of information.

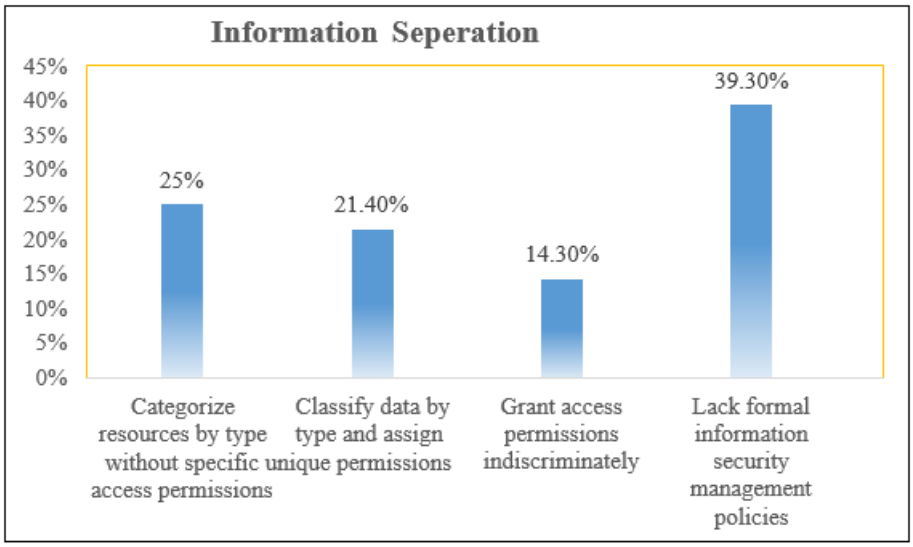

Figure 4: Information Separation

Figure 5 illustrates the significant cybersecurity risks associated with connecting external discs to telecom and banking systems in bosaso. These risks include data loss, virus infection, and unauthorized network intrusions. Survey results indicate concerning attitudes toward these practices within organizations. According to the figure, 35.7% of respondents believe that telecom companies and banks in Bosaso shouldpermit any employee to connect external discs to work computers. An additional 17.9% advocate for even less restrictive access, suggesting that anyone should be allowed to connect external discs to corporate computers. In contrast, 46.4% of respondents report that telecom companies and banks restrict the use of external drives to authorized employees and specific PCs.The survey data reveal a critical gap in cybersecurity practices. Allowing broad access to external discs heightens the risk of malware infections and unauthorized data access, which could compromise sensitive financial information. The substantial support for lenient policies among respondents underscores a general lack of awareness about the potentialrisks. To mitigate these risks, telecom companies and banks should implement stricter access controls for external discs. Policies must limit the use of external drives to authorized personnel only. Additionally, organizations should launch comprehensive cybersecurity awareness campaigns to educate employees about the threats posed by external discs. Adhering to established best

practices and regulations governingexternal drive usage will further enhance protection against data breaches and malware infections.

The survey highlights an urgent need for improved cybersecurity measures concerning external discs withinbanks and telecom companies. Adopting stringent policies and enhancing employee awareness are essential steps in mitigating the risks associated with external discs and safeguarding sensitive information.

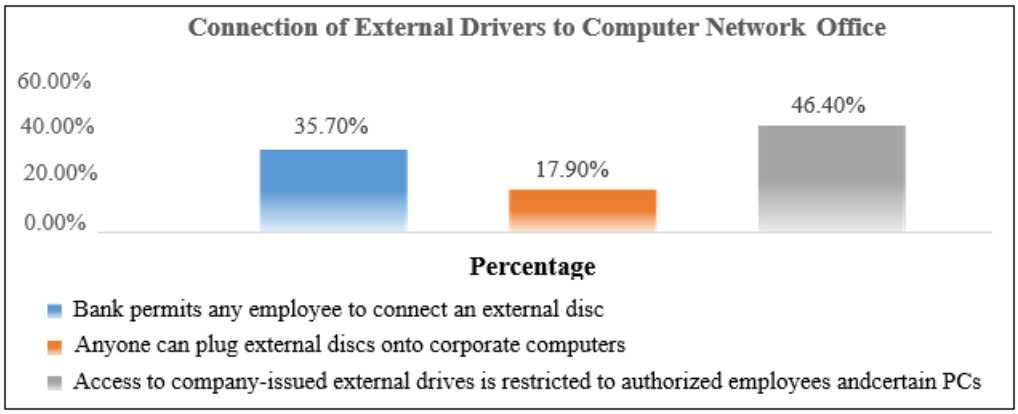

Figure 5: Computer Office Management

Figure 6 provides an analysis of security program coverage based on the survey data presented in Figure 4.10. It assesses the extent to which organizations have adopted security policies for critical systems and practices. The data indicates that 28.60% of organizations have established policies for securing remote access connectivity. This figure reflects a moderate level of preparedness for managing remote work environments, which have become increasingly prevalent. However, 10.70% of respondents have documented protocols specifically for safeguarding core banking systems, revealing a significant vulnerability in protecting crucial financial infrastructure. Moreover, 17.90% of respondents have implemented breach response strategies, which suggests a degree of preparedness for handling security incidents. Nevertheless, this also implies that a majority of organizations may lack comprehensive incident management plans. Similarly, 10.70% have identity theft prevention programs, highlighting a limited emphasis on this critical area of security. The most concerning finding is that 46.40% of respondents lack any documented policies. This substantial percentage underscores a critical gap in formal security practices and indicates an urgent need for comprehensive policy development. The survey data reveal significant disparities in security program coverage among organizations. While some have adopted essential policies,nearly half lack documented procedures, highlighting an urgent need for enhanced security measures. To address these gaps, organizations must develop and implement comprehensive security policies to improve resilience and protect against emerging threats.

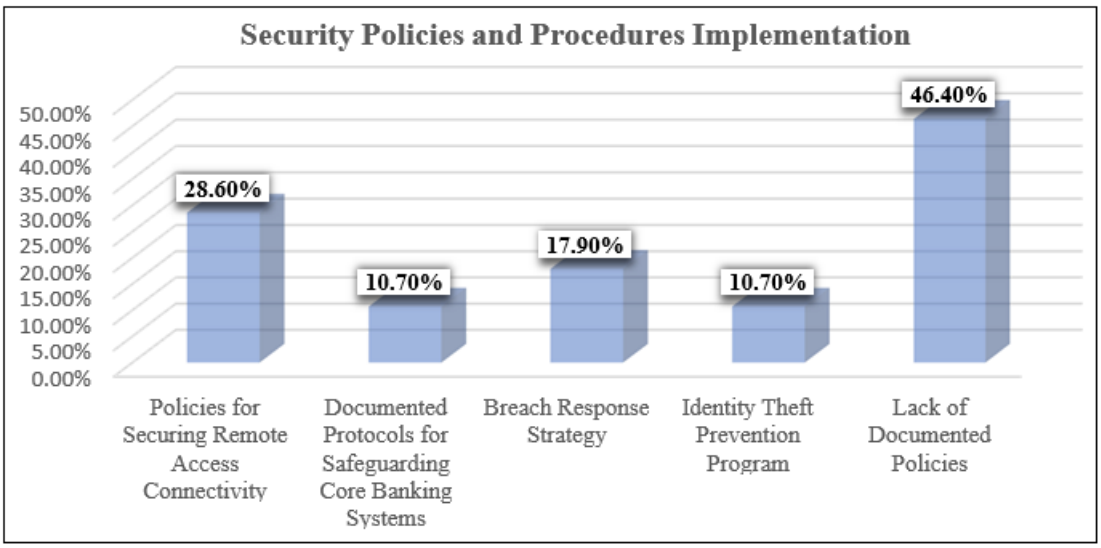

Figure 6: Security Policies and procedures

Effective information security training is vital for equipping staff to address contemporary cyber threats. Figure 7 presents survey data that highlights a significant disparity in the timing of training and awarenessinitiatives across organizations. The data indicate that 42.90% of respondents reported that their organizations last conducted information security training over two years ago. This extended interval without recent training raises substantial concerns about staff preparedness. Outdated training can result inemployees being ill-equipped to recognize and respond to evolving cyber threats such as phishing, whaling, and identity theft, thereby increasing organizational vulnerability. In contrast, 57.10% of

respondents reported that their organizations have implemented training and awareness initiatives within the past two years. This suggests a more proactive approach to cybersecurity, aligning with best practices that emphasizethe importance of regular updates to training programs. Despite this positive trend, the fact that a significant portion of organizations (42.90%) has not conducted recent training underscores a critical gap in maintaining current cybersecurity knowledge. To address these deficiencies, it is essential for organizationsto adopt a more frequent training schedule. Implementing refresher training sessions at least every three months would ensure that employees remain informed about the latest threats and best practices. This approach would enhance organizational resilience by keeping staff up-to-date with evolving cyber threats and practices, thereby reducing the risk of security breaches. Regular updates to training programs are crucial for sustaining a robust cybersecurity posture and effectively mitigating potential risks.

Figure 7: Security Trainings in Telecom and Banks

Understanding the types of cyber-attacks impacting banks is crucial for strengthening cybersecurity measures. Figure 8 provides insight into the frequency and nature of these attacks over the past two years. Nearly 43% of banks reported experiencing computer virus or malware attacks. This substantial percentage highlights a critical area of vulnerability. The prevalence of these attacks underscores the urgent need for enhanced antivirus solutions and malware protection. Banks must invest in advanced security technologiesand implement robust protocols to defend against such threats. DDoS attacks affected 10% of respondents' banks. Although less common than malware attacks, DDoS incidents can still significantly disrupt banking operations. This emphasizes the importance of having effective DDoS mitigation strategies and response plans to ensure service continuity during such disruptions. Phishing and vishing attempts impacted 32% ofbanks, reflecting a notable threat from social engineering attacks aimed at obtaining sensitive information. Banks need to prioritize staff training to recognize and handle these types of attacks effectively, reducing the risk of successful breaches. The 15.10% of respondents who were unsure or lacked information about the attacks indicates a gap in cybersecurity awareness and reporting. Addressing this uncertainty is essential for improving incident response and overall security posture. The data reveals significant cybersecurity challenges for banks, particularly concerning computer virus and malware attacks. Enhancing antivirus measures, improving DDoS defenses, and increasing staff training are crucial steps for mitigating these threats and strengthening telecom and bank security.

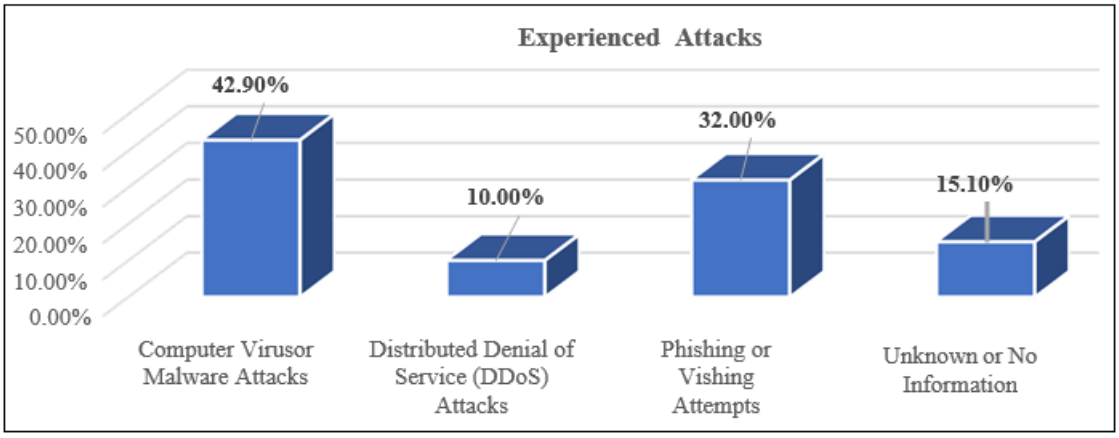

Figure 8: Experienced Attacks

Effective incident response is a fundamental component of an organization's cybersecurity strategy, particularly in the banking sector where the protection of client information is of utmost importance. Figure 9 illustrates a significant disparity in the adoption of security incident response measures among banks. Survey data in figure 9 reveals that 46.40% of respondents reported that their banks have established protocols for managing security incidents involving client information. This statistic suggests that a noteworthy portion of the banking sector is proactive in developing strategies to address and mitigate security threats. Implementing these protocols is essential for minimizing the impact of potential breaches and ensuring a swift response to emerging threats. Despite this, nearly half of the banks, indicated by the remaining 53.60%, havenot yet integrated comprehensive incident response procedures into their cybersecurity frameworks. This indicates a critical gap in the current security practices. Conversely, 53.60% ofrespondents noted that their banks have not implemented security incident response measures for client information. This substantial percentage underscores a significant vulnerability in the sector.The absence of dedicated incident response strategies increases the risk of security breaches and inadequate protection of client data, an issue of particular concern given the increasing frequencyand sophistication of cyber threats. The survey results highlight a pressing need for enhanced incident response strategies within the banking sector. Banks that have yet to adopt comprehensive security incident management practices are at a heightened risk of data breaches and subsequent damages. It is crucial for these institutions to develop and implement robust incident response plans to effectively safeguard client information. Strengthening these measures will not only bolster organizational resilience but also ensure adherence to cybersecurity best practices.

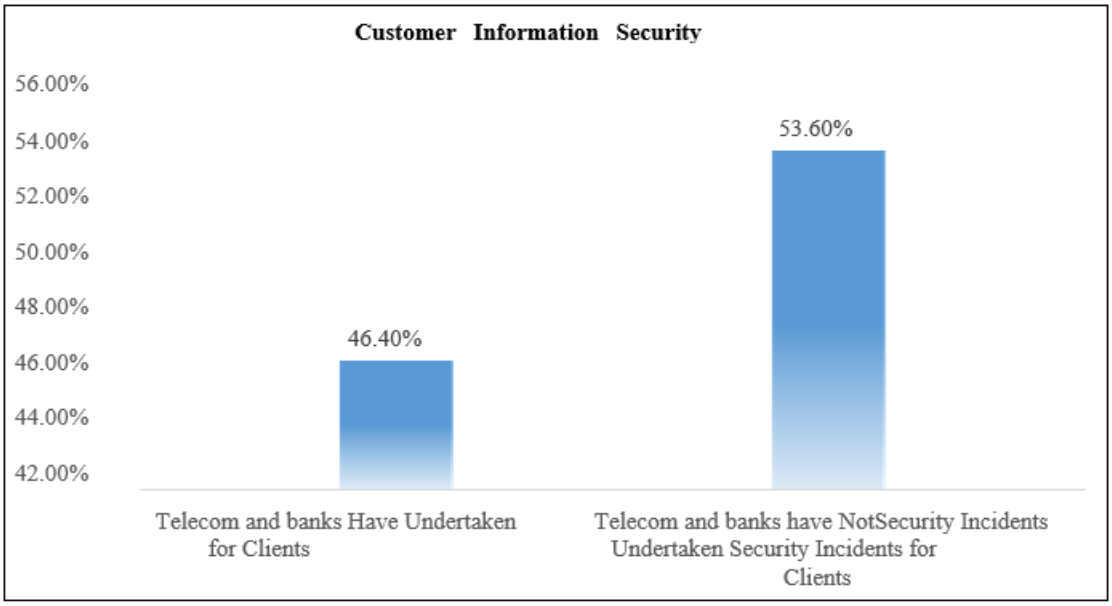

Figure 10 illustrates the divergence in organizational policies concerning third-party data access. Specifically, 39.30% of organizations permit third-party access to their data, whereas a substantialmajority of 60.70% restrict such access. This significant disparity underscores a prevailing trend towards prioritizing data privacy and security. The predominant preference among organizations that prohibit third-party access is indicative of a strategic focus on data protection. This approach likely reflects concerns about potential vulnerabilities associated with external parties, including risks of data breaches, unauthorized use, and challenges in adhering to stringent data protection regulations. Such organizations appear to emphasize safeguarding their data by minimizing exposure to external risks. Conversely, the 39.30% of organizations that allow third-party access may be seeking to capitalize on the benefits of external expertise, outsourcing capabilities, or system integration. For these entities, the potential advantages in terms of operational efficiency and enhanced functionality justify the risks associated with third-party interactions. Nevertheless, organizations that permit third-party access must implement rigorous management protocols to mitigate potential risks. This typically involves the establishment of comprehensive agreements with third parties, stringent security measures, and continuous oversight to ensure compliance withrelevant data protection standards. Overall, the data reveals a predominant inclination towards restricting third-party access, emphasizing a cautious approach to data security and risk management. For those organizations that do engage third parties, the implementation of robust safeguards is essential to balance the benefits of external collaboration with the imperative to maintain data integrity and security. This balance is increasingly crucial in the contemporary data-driven landscape.

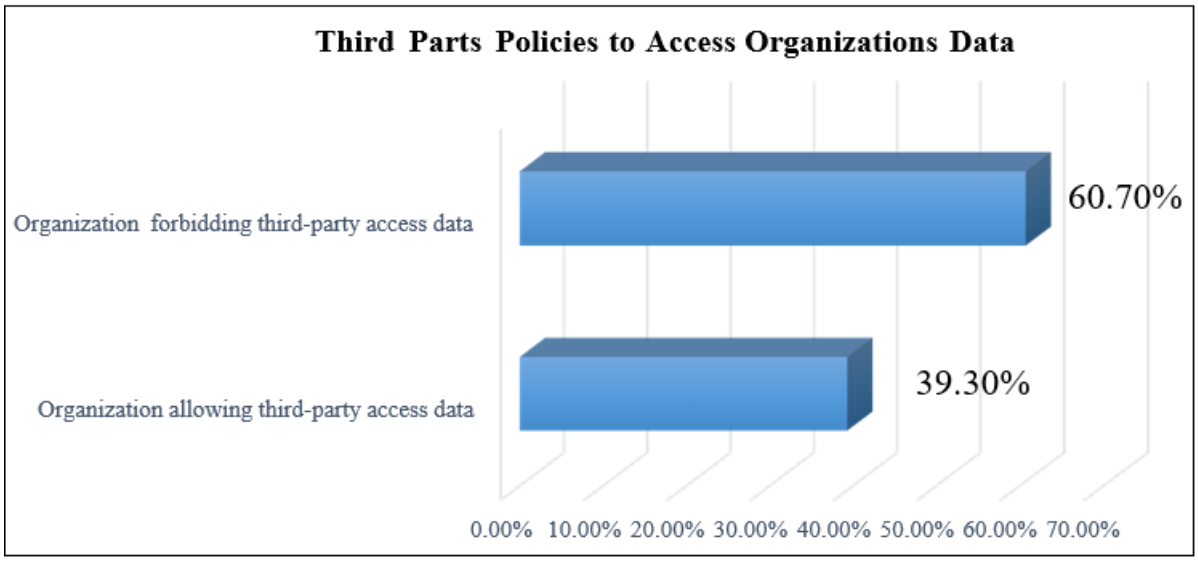

Figure 10: Parts Policies

5. Discussion and Conclusion

The findings from this study highlight significant challenges within the cybersecurity landscape of Bosaso's banking and telecom sectors. A critical issue identified is the lack of robust access control measures. Approximately 46% of respondents reported that access control is not enabled on their computers, indicating a significant vulnerability in safeguarding sensitive financial data. This deficiency in fundamental security measures poses substantial risks to data integrity and confidentiality. Additionally, 40% of respondents acknowledged the presence of access control mechanisms that could be bypassed by workers, underscoring the ineffectiveness of current security measures. Only 14% of respondents indicatedthat access control was both enabled and properly managed, emphasizing the struggle among organizations to implement and maintain effective security practices. The data further revealed that 25% of organizations classify their resources by type but do not delineate specific access permissions, thereby exposing sensitive data to potential threats. Another 21.4% of organizations assign unique permissions to classified data, reflecting a more secure approach; however, this practice is less common. Alarmingly, 14.3% of organizations permit indiscriminate access to resources, posing severe security risks. The absence of formal information security management policies in 39.3% of organizations further exacerbates these vulnerabilities.

5.1 Conclusion

The study concludes that there is an urgent need for Bosaso's telecom and banking institutions to enhance their cybersecurity measures, particularly in improving access control protocols. The low confidence levels among respondents regarding their institutions' cybersecurity postures reflect broader issues of insufficient security practices and awareness. The findings suggest that many organizations in Bosaso struggle to implement and enforce rigorous access control measures, leaving them vulnerable to internal and external threats. To address these challenges, it is crucial for organizations to adopt stricter enforcement of access control policies and ensure proper management and regular reassessment of these measures. Enhancing cybersecurity awareness and training among employees is also essential to mitigate risks and foster a culture of proactive cybersecurity practices. By addressing these deficiencies, Bosaso's private sector can better protect sensitive data and improve overall cybersecurity resilience.

5.2 Implication for Research

The study highlights several key areas that warrant further exploration within the cybersecurity domain, particularly in the context of Bosaso's banking and telecom sectors. The findings reveal critical gaps in access control measures and overall cybersecurity awareness, suggesting that future research should delvedeeper into the factors influencing these deficiencies. One significant implication is the need to investigatethe socio-cultural and organizational factors that impede the implementation of robust cybersecurity practices. Understanding the specific challenges faced by organizations in Bosaso can help tailor more effective strategies for enhancing security measures. Moreover, examining the role of employee training and awareness programs in mitigating cybersecurity risks can provide valuable insights into improving organizational resilience. Additionally, the study highlights the importance of exploring technological solutions that can address the identified vulnerabilities. Research into advanced access control mechanisms,intrusion detection systems, and other security technologies could contribute to developing more secure infrastructures for the banking and telecom sectors in Bosaso. This technological focus can be complemented by studies on the efficacy of current cybersecurity policies and the development of new frameworks that are better suited to the local context. Finally, the research points to the potential benefits of a more collaborative approach to cybersecurity. Future studies could investigate the impact of partnerships between private sector organizations, government agencies, and international cybersecurity bodies on improving security postures. Such collaborations could lead to the sharing of best practices, resources, and knowledge, thereby enhancing the overall cybersecurity landscape in Bosaso.

In summary, the study's implications for research highlight the need for a multifaceted approach that includes socio-

cultural, technological, and collaborative dimensions to address the cybersecurity challengesfaced by Bosaso's private sector.

5.3 Implication for Practice

The study highlights several critical areas for immediate improvement in the cybersecurity practices of Bosaso's banking and telecom sectors. Organizations must prioritize implementing and enforcing robust access control measures to safeguard sensitive information. The current deficiencies, such as the lack of access control on many computers and the ability of employees to bypass existing measures, present significant security risks. Addressing these issues involves adopting stricter access control policies and ensuring that permissions are clearly defined and effectively managed. The absence of formal informationsecurity management policies in many organizations further exacerbates vulnerabilities. Developing and implementing comprehensive security policies are essential steps toward enhancing cybersecurity resilience. These policies should include clear guidelines for information handling, access permissions, and security protocols. Additionally, enhancing cybersecurity awareness and training among employees is crucial. Regular training sessions should be conducted to keep staff updated on the latest cyber threats andbest practices. This approach will foster a culture of proactive cybersecurity practices, reducing the likelihood of security breaches. By addressing these deficiencies, Bosaso's private sector can significantlyimprove its cybersecurity posture, better protecting sensitive data and ensuring organizational resilience against cyber threats.

6. Future Recommendations

The future recommendations based on the study's findings emphasize several critical actions that can enhance the cybersecurity posture of Bosaso's telecom and banking sectors. Firstly, it is imperative to establish comprehensive and formal information security management policies across organizations. Thesepolicies should be designed to address the identified gaps in access control and data protection, ensuring that robust mechanisms are in place to safeguard sensitive information. Organizations should prioritize the implementation of rigorous access control measures. This includes enabling access control on all computers, regularly updating and managing these controls, and ensuring that they cannot be easily bypassed by employees. Additionally, there should be a clear delineation of access permissions for differenttypes of data to minimize the risk of unauthorized access and potential data breaches.Furthermore, enhancing cybersecurity awareness and training programs is essential. Regular training sessions should be conducted to keep employees informed about the latest cyber threats and best practices in mitigating theserisks. This will help in cultivating a culture of proactive cybersecurity within organizations.

Investment in advanced cybersecurity technologies is also recommended. Organizations should adopt state- of-the-art solutions for malware protection, intrusion detection, and incident response. These technologies should be complemented by well-defined protocols for managing and responding to security incidents, ensuring that organizations can swiftly and effectively address any breaches that occur. Lastly, continuous assessment and improvement of cybersecurity measures are crucial. Organizations should regularly review their security policies and practices, incorporating feedback and adapting to emerging threats and vulnerabilities. By maintaining a dynamic and responsive approach to cybersecurity, Bosaso's telecom and banking sectors can significantly enhance their resilience against cyber-attacks. These recommendations, if implemented effectively, will not only strengthen the cybersecurity infrastructure of individual organizations but also contribute to the overall security and stability of the private sector in Bosaso.

Acknowledgements
I would want to thank the following people from the bottom of my heart: To **Asia e University** and **Prof. Dr. Fazilah Che Fauzi**, the academic coordinator for the school of information and communication technology, for their unwavering support during my studies and for serving as an inspiration to me with herendurance and vast knowledge. Her advice was helpful to me throughout the entire research and writing process for my project paper. To my supervisor, **Prof Dr. Titik Khawa Abdul Rahman** for her contribution and advice that become a key success to this paper; and to my **Dear father Abdirisak** Buraale Farah and mom **Muhubo Mohamed Ahmed**, for their encouragements and companion along the journey.

References

[1] Angraini, M. (2019). Data integrity in information systems. *Journal of Information Security*, *10*(3),145-159.
[2] Angraini, M. (2019). Data integrity in information systems. *Journal of Information Security, 10*(3),145-159.
[3] Bleeping Computer. (2023). Ransomware attacks and their impact. Retrieved from https://www.bleepingcomputer.com/ransomware
[4] Bussell, J. (2013). The evolution of cyberspace regulation. *Cyberspace Review, 12*(1), 22-34.
[5] Cisco. (2020). The state of cyber security. Retrieved from https://www.cisco.com/security-report
[6] David, M. (2008). The consumer impact of cybercrime. *Cybersecurity Journal, 5*(2), 77-85.
[7] Europol. (2022). Data theft and its global impact. Retrieved from https://www.europol.europa.eu
[8] FireEye. (2021). The landscape of cyber espionage. Retrieved from https://www.fireeye.com/cyber-espionage
[9] Gagliardone, I., & Sambuli, N. (2015). Cyber security in Somalia: Challenges and solutions. *AfricanJournal of Information Security, 8*(4), 195-208.
[10] Gibson, W. (1984). *Neuromancer*. Ace Books.
[11] HackerOne. (2021). Data interception techniques. Retrieved from https://www.hackerone.com
[12] IS Forum. (2011). The importance of cyber security for businesses. Retrieved from https://www.isforum.com
[13] Kaspersky Lab. (2015). Security threats report 2015. Retrieved from https://www.kaspersky.com/security-report
[14] Kaspersky Lab. (2021). Trends in cyber extortion. Retrieved from https://www.kaspersky.com/cyber-

extortion
[15] McAfee. (2020). The state of credit card fraud. Retrieved from https://www.mcafee.com/credit-card-fraud
[16] Michael, J. (2011). Protecting data confidentiality. *Information Security Journal, 16*(1), 45-53.
[17] Monica, R., Smith, J., & Anderson, B. (2014). Economic impacts of cyber breaches. *Journal of Financial Security, 9*(2), 112-126.
[18] Norton. (2011). The economic costs of cybercrime. Retrieved fromhttps://www.norton.com/cybercrime
[19] Rouse, M. (2019). The importance of cyber security in the digital age. *Tech Journal, 15*(4), 34-45.
[20] Richard, J. (2019). Network security and organizational resilience. *Journal of Network Security,21*(3), 78-89.
[21] Smith, R. (2004). Consumer trust and online transactions. *E-Commerce Journal, 8*(3), 123-139.
[22] Symantec. (2020). Digital fraud and social engineering techniques. Retrieved from https://www.symantec.com/digital-fraud
[23] Tonggal, H. (2020). Implementing effective information security measures. *Cybersecurity Review, 11*(2), 56-69.
[24] Venkat, S. (2016). Network crimes and prevention strategies. *Journal of Cyber Law, 14*(1), 89-103.
[25] Verizon. (2023). Data modification and its impact on organizations. Retrieved from https://www.verizon.com/data-modification
[26] Kumar, A. M. (2015). A review of security and data hiding techniques. *International Journal ofInventive Engineering and Sciences (IJIES)*, 31.
[27] Jama, A. Y. (2015). Survey on data modification attacks. *International Journal of Scientific & Engineering Research, 6*(2), 778-781.
[28] Friedman, A. W. (2013). *Cyber security and cyber war: What everyone needs to know?*
[29] Augenbaum, S. (2019). *The secret to cyber security: A simple plan to protect your family andbusiness from cybercrime.*
[30] Brotherston, A. B. (2017). *Defensive security handbook: Best practices for securinginfrastructure.*
[31] CERT-Somalia. (2018). Retrieved from http://som-cert.org/about-us/
[32] Hare, H. (2007). ICT in education in Somalia. In *Survey of ICT and education in Africa: Somalia country report*.
[33] Lancaster, H. (2018). *Somalia - Telecoms, mobile and broadband - Statistics and analyses*. Buddecomm.
[34] Nuh, M. (n.d.). *Literature review of technology diffusion in Somalia*. Retrieved from https://www.academia.edu/96195642/Literature_Review_Of_Technology_Diffusion_In_Somalia