Volume 9, Issue 7, July – 2024 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL264

Factors Affect Cyber Security Readiness and Performance of SMEs: A Case Study of Mogadishu, Somalia

Sayid Ali Abubakar Sheik Ahmed[1]
Computer Science & IT
Asiae University
Selangor, Malaysiya

Mohamed Adam Isak Abdirahman[2]
Computing Sciences
Darul Hikmah University (DHU)
Mogadishu, Somalia

Abstract:- The incorporation of new digital technologies into the small business environment has led to the emergence of new potential threats and risks. The impact of cybercrime on the operational effectiveness and performance of business entities is a major challenge. Each year, billions of dollars are lost to cybercrime. In order to address this issue, SMEs have invested heavily in cyber-security protocols. In this study, we aimed to analyze the various factors that influence cyber security readiness among SMEs in the greater Mogadishu area. Specifically, we looked at how management support and resource factors, as well as regulatory factors, affect cyber security readiness among small and medium enterprises in Somalia. The methodology of the study was based on a positivistic approach with descriptive research. The sample size was all operational SMEs in the city of Mogadishu. The respondents were either ICT managers or IT security or other IT professional. A structured research questionnaire was employed to facilitate the collection of data. This was supplemented by the use of Google forms and, where feasible, actual data collection. The analysis of the data was conducted through the utilization of descriptive metrics, correlations and regression, which were presented in the form of tables. The findings of the study revealed a positive relationship between the level of management support, resource and regulatory factors in relation to cyber Security readiness and performance in the city of Mogadishu, indicating a positive correlation. The overall regression showed that the above-mentioned factors play a significant role in the cyber Security status of the SMEs in Mogadishu. In order for SMEs to become more cyber security prepared, the findings of the study indicate that organizations must be adequately prepared to allocate significant financial and technological resources to cover the considerable expenses associated with the pursuit of cyber security status. The study also advises managers to coordinate security choices with organizational objectives and capabilities to lessen imbalances that might prevent the effective application of cyber security measures. Finally, the study recommends that SME policy makers should assess the readiness of the industry and create a set of norms and standards that all firms can meet, as this would support cyber security preparedness and performance.

Keywords:- *Cyber Security Readiness and Performance, Management Support, Resource Factors, Regulatory Factors, Small Medium Enterprises. (SMEs)*

I. INTRODUCTION

Significant advances in digital technologies, devices and interconnectivity have benefitted organizations in a variety of ways, including improved system accessibility, increased speed of communication, improved efficiency and reduced operating costs. Digital technologies offer organizations new market opportunities and higher-quality products. However, organizations undergoing digital transformation continue to face the risk of information technology (IT)/cyber threats and attacks on their assets.

This paper defines "cyberspace" as the virtual environment, specifically the electronic medium used for online communication, encompassing various purposes from business to leisure, and highlights its presence in various settings, including virtual meeting rooms.(if somewhat theoretical) way. (Techopedia, 2022).

This research explores cyber-security, a crucial process involving policies, procedures, strategies, threat management, engagements, education, and best practices to protect a company's infrastructure and digital assets from known and unknown threats. Effective cyber-security can boost innovation, increase sales, and lead to more valuable organizations.(Lloyd, 2020).

Cybercrime is a criminal activity involving the use of computers or networks for criminal activities, targeting individuals, groups, or countries, and using various techniques to investigate suspected devices.(CyberTalents, n.d.). The researcher investigated the use of connected devices in facilitating and committing illegal activities on technological devices used by growing SMEs.

This paper reviews previous studies, develops a research model and hypotheses, describes the research method, tools, and techniques, presents findings, implications, and conclusions, and concludes with recommendations for future work.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL264

II. LITERATURE REVIEW

This review examines factors affecting SMEs' cyber security preparedness and performance in Mogadishu, focusing on management support, resource factors, and regulatory factors, and highlights the growing dependence on digital technology.

- *Cyber Security Readiness and Organizational Performance*

The study indicates that an organization's security performance significantly impacts its cyber-security preparedness, consistent with a previous study by (Angst et al., 2017) Organizations that enhance their cyber security preparedness improve security performance by reducing data breaches, establishing a strong security reputation, enhancing internal process security, and constructing a robust system.

- *Factors Affect Cyber Security Readiness and Performance of SMEs*

This section examines the factors affecting small and medium-sized enterprises (SMEs) in Mogadishu, Somalia, including cyber securityreadiness and performance. It discusses the increasing use of digital technologies, increasing cyber threats, and the impact of management support, resource factors, and regulatory factors on SMEs' cyber securityreadiness.

- *Management Support and Cyber Security Readiness*

Management support in Mogadishu, Somalia, is crucial for promoting a strong cyber security culture within an organization. Research shows that SMEs with strong leadership commitment have higher preparedness and better performance. Understanding this correlation is essential for enhancing their cyber securityposture.

The study examines the impact of management support for audit functions on an organization's capacity to identify, reduce, and address cyber-risks for the first time. (Alina et al., 2017). The Deloitte IIA model assesses cyber-security readiness, emphasizing the crucial role of managers in creating a safe environment, anticipating risks, and ensuring quality assurance. According to (Knapp et al., 2005) Top management significantly improves cyber security readiness by promoting employee training, fostering a security-conscious culture, and enforcing security policy compliance, leading to increased prevention efforts in organizations.

Barton et al. (2016) found top management commitment is essential for implementing security technologies and maintaining policies.(Catota et al., 2019) Ecuadorian financial institutions face budget constraints in addressing security incidents and implementing controls. To improve cybersecurity, they should educate executives on data protection and invest in threat detection technologies.

Top management's commitment to cyber security significantly influences employees' attitudes towards the organization's security policies and strategies, thereby aligning with institutional theory's mimetic nature..(Daud et al., 2018).According to (Hsu et al., 2012) The successful adoption of IT systems security is attributed to the involvement of top management in information security management. Furthermore, According to (Puhakainen & Siponen, 2010) Top management's commitment to cyber security is assessed through their adherence to security policies and guidelines. According to (Kankanhalli et al., 2003) “Top management can improve cyber security by actively participating in the development of IS security policies.

Institutional theory research emphasizes the crucial role of organizational skills, particularly IT and cyber securityskills, in enhancing cyber security within organizations.

According to (D’Arcy et al., 2014), Regular training and education programs enhance cyber securityby teaching current technical competencies to an organization's workforce, addressing the complexities of security and meeting institutional theory requirements. While (Ravichandran & Rai, 2000)) Studies highlight the significance of organizational skills in managing cyber security, emphasizing the need for adequate resources for effective training and awareness programs.As (AlEnezi, 2019) Expert employees improve organizations by implementing effective cyber-attack strategies and enhancing readiness, while empowering and increasing their knowledge positively impacts their cyber securityreadiness.

According to (Mose, 2019) Human factors significantly impact cyber security, with changing user behavior altering organizational security culture. Staff training and awareness are crucial for cyber security readiness, ensuring best practices are implemented.

- *Resource Factors and Cyber Security Readiness*

Resource factors encompass the availability and allocation of resources, including financial, technical, and human resources, dedicated to cyber security practices in SMEs. This variable will examine whether SMEs in Mogadishu have adequate resources to implement robust cyber security measures. Technology readiness involves optimism, invention, flexibility, efficiency, and thought leadership, while preparedness involves fear, confusion, anticipation, doubt, and skill questions, both crucial for successful technology use.

(Kong et al., 2012) Technological factors significantly influence an organization's readiness to maintain its cyber infrastructure and services, enhancing its readiness against cyber-attacks. Enhancing readiness involves increasing IT professionals, tools, and resources.

According to (Chang & Chen, 2021) The researcher plans to create a model to analyze factors affecting an organization's cyber security and technology readiness, focusing on its impact on small businesses' performance.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL264

Small and medium-sized enterprises (SMEs) are vital components of larger organizations' supply chains, and a successful cyber-attack could significantly disrupt the entire industry.(Rezaei et al., 2015). Data breaches and cyber-attacks significantly impact both large and small organizations, as extensively documented in news and scholarly research. (Gafni & Pavel, 2019). Larger organizations have IS professionals to mitigate risks and counter data breaches, while SMEs lack such structures, awareness, and cyber securityreadiness..(Neri et al., 2022).According to (Bell, 2017) Cyber security challenges SMEs face similarly to larger organizations, but their response to threats varies due to their lack of expertise and resources. The Ponemon Institute's 2012 A 2016 study found that UK small enterprises face challenges in cyber securitypreparedness due to a lack of technical resources and compliance with regulations regarding firewalls.

Utilizing the theory of human–organizational–technological (HOT),A recent study conducted by (Kumar et al., 2020) The study highlights the importance of technology, regulatory compliance, senior management roles, information security requirements, technical professionals, and employee morale in ensuring long-term security in small and medium-sized enterprises.

SMEs in Africa face challenges like power shortages, capital constraints, management skills lack, information corruption, and lack of support from governments, neglecting their vital role in economic growth..(Muriithi, 2017). Somalia faces a significant cyber security issue as cybercriminals are targeting government assets for destruction, data extraction, and personal information collection, with financial gain and intelligence sharing as objectives. Somalia faces a significant cyber security crisis, with cybercriminals targeting government assets, disrupting infrastructure, extracting information, and stealing personal data for financial gain or intelligence purposes. (source: Sambuli et al. 2015)

- *Regulatory Factors and Cyber Security Readiness*

Regulatory factors pertain to the influence of laws, regulations, and government policies on cyber security practices in SMEs. This variable investigates the extent to which compliance with cyber security regulations impacts the readiness and performance of SMEs in Mogadishu, Somalia.

Government rules significantly impact e-business security and cyber security architecture. Deterrence theory suggests they help firms maintain information security, set regulations, protect online transactions, promote visibility, and increase preparedness for cyber threats.(Wall et al., 2016).Deterrence theory emphasizes government assistance in enhancing enterprise cyber security, as it informs corporations about cyber-attacks, implements countermeasures, and enhances organizational readiness by raising cyber security knowledge.(Maow, 2021) According to (Kenneth J. Knapp et al., 2006), Governments are tasked with promoting information security by implementing cyber security initiatives.

The study on Turkey's cyber resilience suggests a critical infrastructure protection program, focusing on collaboration and updates to anticipate threats. It emphasizes identifying risks, developing cooperation routines, and executing cyber-security activities. Enhanced cyber readiness, particularly in SMEs, is linked.

(Nieles et al., 2017) A cyber securitypolicy is a set of rules, guidelines, and best practices aimed at safeguarding critical infrastructure and sensitive data, requiring employees to adhere to incident procedures. According to (Daniel, 2015) The text emphasizes the significance of clear communication of security policies among all employees, as it helps protect data and minimizes human error risk. According to (Assefa & Tensaye, 2021) A lack of a cyber-security policy indicates a lack of understanding of sensitive information, awareness of potential vulnerabilities, and preparedness to respond to cyber-attacks..(Yliopisto, 2017) The text emphasizes the significance of clear and effective communication of cyber securitypolicies for employee commitment, highlighting the potential negative impact of lack of knowledge on compliance and organizational security. This study focuses on the cyber security readiness of organizations, assesses the relevance of factors affecting cyber security identified from previous studies, and investigates the impact of cyber security readiness on three aspects of organizational performance.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL264

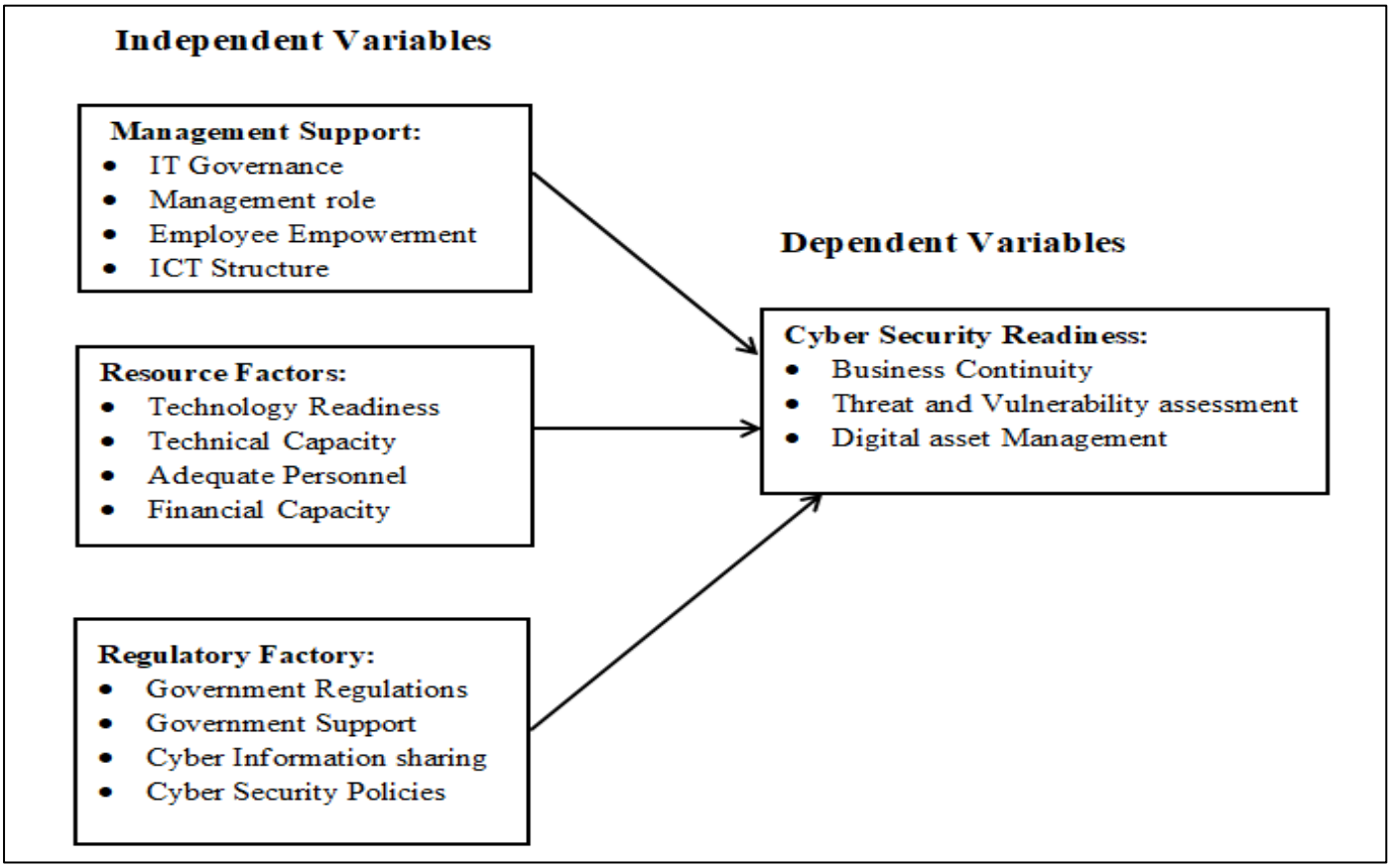

Fig 1 Cyber Security Readiness Model

III. RESEARCH MODEL AND HYPOTHESES

We create a cyber security preparedness model (Fig. 1) based on the TOE framework's eleven components and environmental settings. Because of their distinct limitations, the three theories are used in tandem in this study inside the holistic TOE framework to give a more thorough understanding of the variables influencing enterprises' cyber security readiness.

Within the technical context of the TOE framework, this study applies institutional theory to investigate the impact of management support on an organization's security preparedness. Institutional theory is also used in the TOE framework's Resource Factors to analyze how top management support, organizational skills, and organizational culture affect an organization's security preparedness. Within the external Regulatory Factors of the TOE framework is used to understand the impact of collaboration with competitors and supplier/partner relationships on an organization's security readiness to understand the impact of government regulations, government support, and industry standards on such readiness.

Cyber security preparation positively impacts organizational security performance, which in turn improves financial and other performance. Improved security performance can be evaluated using financial metrics like sales, earnings, and market share, suggesting IT can enhance income and profit ratios. Non-financial performance is influenced by a company's market position, brand image, and reputation, with customer acquisition and retention being key metrics. Security performance, crucial for a strong reputation, impacts both financial and non-financial performance. Other factors like management and employees also contribute to organizational performance.

Management support refers to the provision of assistance, resources, and guidance by senior management or leadership to facilitate the effective functioning of lower-level managers and employees within an organization. Top management refers to the highest level of executives within an organization who are responsible for making strategic decisions and setting the overall direction of the company.

- **H1:** Effective IT governance helps organizations to optimize the value derived from IT investments, manage risks, enhance decision-making, and ensure accountability and transparency in the use of technology resources.
- **H2:** management roles refer to positions within an organization that are responsible for overseeing the planning, implementation, and maintenance of information technology systems and services. These roles are critical for ensuring that IT resources are aligned with business objectives, effectively utilized, and properly managed.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL264

- **H3:** Employee empowerment can lead to various benefits for organizations, including increased employee engagement, motivation, and job satisfaction, improved decision-making and problem-solving, enhanced creativity and innovation, and ultimately, better organizational performance and competitiveness.

Resource factors in IT encompass various elements that are essential for the effective functioning and success of IT initiatives within an organization. These elements include technology readiness, technical capacity, adequate personnel and financial capacity. These resource factors, organizations can optimize their IT investments, enhance operational efficiency, mitigate risks, and leverage technology to achieve their business objectives.

- **H4:** Technology readiness refers to an organization's or individual's preparedness to adopt and effectively utilize a particular technology.
- **H5:** Technical capacity refers to an organization's ability to effectively utilize and leverage technical resources, knowledge, and expertise to achieve its goals and objectives.
- **H6:** "Adequate personnel" refers to having a sufficient number of qualified individuals with the necessary skills, knowledge, and experience to fulfill the requirements of a particular role or task within an organization.
- **H7:** Financial capacity refers to an organization's ability to manage its financial resources effectively to achieve its goals and objectives. It encompasses the organization's ability to generate revenue, manage expenses, allocate funds strategically, and maintain financial stability and sustainability over time.

Regulatory factors refer to laws, regulations, policies, and standards established by governmental bodies, industry organizations, or other regulatory authorities that influence the operations, practices, and behaviors of businesses, organizations, and individuals within a particular industry or jurisdiction.

- **H8:** Government regulations play a crucial role in shaping economic and social outcomes, providing a framework for SMEs, organizations, and individuals to operate within.
- **H9:** Government support refers to various forms of assistance, incentives, funding, or services provided by governmental authorities to individuals, Small Medium size businesses, organizations, or communities to promote economic development, social welfare, or public welfare objectives.
- **H10:** Cyber information sharing refers to the practice of exchanging information and intelligence related to cyber security threats, vulnerabilities, incidents, and best practices among SMEs, organizations, government agencies, industry groups, and other stakeholders.
- **H11:** Cyber security policies are a set of guidelines, rules, and procedures established by organizations like SMEs to protect their information systems, networks, and data from cyber threats, vulnerabilities, and attacks.

IV. METHODOLOGY

Our study examines the cyber security readiness and performance of SMEs in Mogadishu, Somalia at the organizational level by focusing on different organizational aspects. A quantitative approach is adopted to investigate organizational readiness to combat cyber-attacks and the relationships between the model constructs and test the model hypotheses. A survey was developed as a quantitative method to test the model hypotheses.

➢ *Target Population*

The respondents were chosen using a stratified random sampling approach. Mogadishu's SMEs were separated into categories according on their industrial type or size. A sample was randomly drawn from each subgroup to ensure representativeness and reduce bias. The research divides the complete study population, which is divided into 15 enterprises. The investigation was carried out in three stages, involving ICT managers, IT security professionals, and other IT professionals. In order to achieve the desired margin of error, reduce non-response bias and guarantee a representative sample size, it is necessary to expand the sample size. However, this study used stratified sampling due to the small sample size and the need to significantly increase the response rate, which led to better response rates for all 15 small and medium-sized businesses (SMEs) in Mogadishu.

Sample size is defined as number of respondents that represent the population. Sample size refers to the number of respondents in a study and the number of respondents is often divided into sub-groups based on demographics like age, gender**, location**, etc. This means that the total sample size represents the whole population. Therefore, the sample size should be taken into consideration when conducting research. The population size was 140 but were obtained 118 and the focus of the study was on ICT managers and IT security professionals as well as other IT professionals within SMEs in Mogadishu, Somalia.

➢ *Questionnaire Procedure*

In order to gather the required information to address the Research Questions a questionnaire has been developed. The questionnaire was delivered to the selected ICT managers, IT security professionals, and other IT professionals of the selected fifteen Small Medium sized Enterprises as discussed already in target population and sampling section. The survey was gathered between jully 2023 and September 2023. A number of criteria were set for the participants, which included:

- ICT managers or IT experts in the SMEs were targeted.
- Preference was given to IT security professionals.
- And other IT professionals were also included.

The questionnaire is intended to offer a brief explanation and summary on the importance of research for Somali SMEs, with there being no amount or coercion or there being no attempt to influence the results in any way whatsoever.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL264

➢ *Questionnaire Development*

Survey method was used to complement the case study research in terms of getting possibility to generalization. A survey is conducted about 15 SMEs in Mogadishu Somalia. A comprehensive questionnaire designed to cover Cyber Security readiness and performance, the current state of SNEs in Somalia, proposing Cyber security readiness in the Somali SMEs. Studying factors that influence SMEs, The study adapted the questionnaire of those sources and references shown in Table below.

Table 1 Measurement Factors

Question. Constructors/ factors	Number of sub Questions	factors source/Reference
Demographic and SMEs information	5	Researchers
Management Support	8	(Alina et al., 2017).
Resource Factors	6	(Kumar et al., 2020)
Regulatory Factors	6	(Nieles et al., 2017)

The respondents were asked to measure the construct items using a five point Likert scale (1 = 'strongly disagree', 2 = 'disagree', 3 = 'neutral', 4 = 'agree', 5 = 'strongly agree'). The respondents were also asked to provide demographic data, Management Support, Resource Factors, Regulatory Factors, and Cyber Security Preparedness and Performance. Before starting the survey data collection process, the survey items were pre-tested in a pilot study of 10 IT professionals conducted in April 2023. Pilot studies improve survey quality by providing feedback from different perspectives to mitigate issues that may arise during the actual survey data collection process.

➢ *Quality Assurance of the Research*

The research tested a questionnaire with SMEs in Mogadishu to ensure accuracy, and based on pilot feedback, the questionnaire was improved for better results. According to Bryman (2016), research validity refers to the reliability of inferences made by researchers based on the study's design and information. It includes internal and external validity, with internal validity affecting reproducibility and external validity involving analysis tools like descriptive and correlation analysis. A pilot study is conducted to ensure understanding, comfort, and importance of questions, with feedback from the pilot helping to create the appropriate flow of questions.

The study will use statistical techniques like Descriptive Statistics, Correlation Analysis, and Multiple Regression Analysis to evaluate the correlation between independent variables and cyber-security preparedness and performance of SMEs in Mogadishu. The study used IBM SPSS and multiple regression analyses to analyze data on management support, resource availability, and regulatory aspects of SME cyber-security readiness in the Mogadishu region of Somalia. Descriptive statistics (DTS) were used to categorize and compare data.

V. DATA ANALYSIS OF DEMOGRAPHIC CHARACTERISTICS

The researchers demonstrated here the following demographic information: The respondent's gender, age, education, the job title of the respondent in the selected SMEs, the working experience of the respondent and the participant's frequency of each responded Somali SMEs. The researchers will also demonstrate the descriptive statistics such as standard deviation, mean, percentage and frequency to demonstrate and evaluate the representativeness of the sample and the characteristics of the survey data. These items of the survey statistics were tabulated, summarized, and reported.

➢ *Gender of the Respondent*

In terms of which gender the respondent is, the majority of the respondents were male and accounted for 80.5%. 19.5% of the respondents were female that question as depicted in Table 2.

Table 2 The Gender of the Respondent

Sex of the respondent.					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	23	19.5	19.5	19.5
	Male	95	80.5	80.5	100.0
	Total	118	100.0	100.0	

➢ *Group of the Respondent Age*

In terms of the age of the respondents, the majority of the respondents were in range 24-28 years old and accounted for 61.9% whereby 18.6 % of the respondents were in range 28-32 and 13.6% were in range 32-36 and 4.2 % of the respondents were 36 and 40 and 1.7% of the respondents were 44 or above as depicted in Table 3.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL264

Table 3 The Group of the Respondent Age

Age of the Respondent					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	24-28	73	61.9	61.9	61.9
	28-32	22	18.6	18.6	80.5
	32-36	16	13.6	13.6	94.1
	36-40	5	4.2	4.2	98.3
	Missing	2	1.7	1.7	100.0
	Total	118	100.0	100.0	

➢ *The Education Level of the Respondent*

In terms of the education level of the respondents, the majority of the respondents holds bachelor degree and accounted for 63.6 % whereby 28.4% of the respondents hold master degree and 31.4 % and 1.7 % of the respondents hold PhD, Diploma and secondary degree as depicted in Table 4.

Table 4 The Level of Education of the Respondent

Level of Education					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Secondary	2	1.7	1.7	1.7
	Diploma	2	1.7	1.7	3.4
	Bachelor	75	63.6	63.6	66.9
	Master	37	31.4	31.4	98.3
	PhD	2	1.7	1.7	100.0
	Total	118	100.0	100.0	

➢ *Marital Status of the Respondents*

In terms of the marital status of the respondents, the majority of the respondents were single and accounted for 55.1 % whereby 44.9 % of the respondents were married as depicted in Table 5.

Table 5 the Respondent's Marital Status

Respondent's Marital Status					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Single	65	55.1	55.1	55.1
	Married	53	44.9	44.9	100.0
	Total	118	100.0	100.0	

➢ *The Years of Experience of the Respondent*

In terms of the experience years of the respondents, the majority of the respondents have years in their experience between less than 5 years and accounted for 41.5 % whereby 36.4 % of the respondents have years in their experience between 5-10 years and 16.9 % of the respondents have 10-15 years' experience and 3.4 % of the respondents have 21 and above years' experience as depicted in Table 6.

Table 6 The Years of Experience of the Respondent

The Years of Experience of the respondent					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less than 5 years	49	41.5	41.5	41.5
	5-10	43	36.4	36.4	78.0
	10-15	20	16.9	16.9	94.9
	15-20	2	1.7	1.7	96.6
	21 and above	4	3.4	3.4	100.0
	Total	q118	100.0	100.0	

➢ *Correlation Analysis*

The study aimed to analyze the impact of management support, governing factors, and resource factors on cyber-security performance and readiness, using the Spearman correlation method.

The study analyzed the impact of management support on cyber-security performance and readiness, finding that it significantly and moderately influences this readiness. (r =.563, p.0005).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL264

The second study assessed the impact of resources on cyber-security performance and preparedness, finding that resources had a positive and statistically significant influence. (r =.395, sig =.000.0005).

The study aimed to assess the impact of regulatory factors on cyber-security performance and readiness, finding a moderately positive and significant effect.(r = 408, sig =.000.0005).

Table 7 Correlation Matrix

			CSR	MSF	RF	RF
Spearman's rho	Cyber Security Readiness	Correlation Coefficient	1.000	.563**	.395**	.408**
		Sig. (2-tailed)	.	.000	.000	.000
		N	117	117	117	117
	Management Support	Correlation Coefficient	.563**	1.000	.575**	.483**
		Sig. (2-tailed)	.000	.	.000	.000
		N	117	117	117	117
	Resource Factors	Correlation Coefficient	.395**	.575**	1.000	.438**
		Sig. (2-tailed)	.000	.000	.	.000
		N	117	117	117	117
	Regulatory Factors	Correlation Coefficient	.408**	.483**	.438**	1.000
		Sig. (2-tailed)	.000	.000	.000	.
		N	117	117	117	117

**. Correlation is Significant at the 0.01 Level (2-tailed).

➢ *Regression Analysis*

The study examines the impact of resources, regulations, and management support on cyber-security readiness and SME performance in Mogadishu, Somalia, using regression analysis.

Table 8 Overall Regression Summary

Model		R square	Adjusted R square	Std Error of estimate
1	651[a]	.424	.408	59197

- The aforementioned model predicts (Constant) 42.4% of the variation in SMEs' cyber-security preparedness. Management support, resource availability, and regulatory variables are among the predicted variables.

Table 9 Overall ANOVA Summary

Model	Sum of square	Df	Mean Square	F	Sig
1 Regression	29.115	3	9.705	27.695	000[b]
Residual	39.598	113	.350		
Total	68.712	116			

- Dependent Variable: Cyber security readiness
- The study examined consistency, managerial support, resource considerations, and regulatory issues, with ANOVA tests revealing a significant correlation between these variables. With an F-value of 27.695 and a Sig of.00005. The study found that Management Support, Resource Factors, and Regulatory Factors significantly and positively influenced the Cyber Security preparedness and performance of SMEs in Mogadishu, Somalia. The regression analysis findings are displayed below.

Table 10 Overall Regression Coefficients

Model	Unstandardized Coefficient		Standardized Coefficient	T	Sig
	B	Std Error	Beta		
1 (constant)	.840	.334		2.517	.013.
Management support	.547	.102	.513	5.383	.000
Resource factors	.045	.111	.038	.406	.685
Regulatory factors	.200	.101	.176	1.989	.049

- Dependent Variable: Cyber Security readiness Y = .840+ $.547X^1$ + $.045X^2$ + $.200X^3$ + .334

A study was conducted to determine the impact of management support on cyber-security readiness of small and medium-sized enterprises (SMEs) in Mogadishu, Somalia. The results indicated a significant coefficient of management support (.547 X 1,.000 <.05), indicating that a change in management support would result in an increase in cyber-security readiness of.547.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL264

A study was carried out in order to analyze the influence of resource determinants on the cyber-security preparedness and performance of SMEs in Mogadishu, Somalia. The research found a strong resource factor coefficient (.045 X 2,.685 X.05). This means that changing resource factors will result in a.045 rise in cyber-security preparedness.

To analyze the influence of regulatory considerations on small and medium-sized companies' (SMEs) cyber-security preparation in Mogadishu, Somalia. The findings revealed a statistically significant regulatory factor coefficient (.200j3;.049 =.05), suggesting that a change in regulatory factors will boost cyber-security readiness by.200.

VI. DISCUSSION OF THE FINDINGS

This section provides an analysis of the results of the study, which are presented according to the objectives of the study andare corroborated by empirical evidence. The study discovered a significant relationship between managerial support, resource management, regulatory factors, and cyber-security performance. The findings suggest that a firm that is able to effectively manage resources, utilize management support and review the regulatory environment can enhance its cyber-security posture. As mentioned in the findings above, the ability of organizational management to support policy and process change to meet regulatory recommendations and compliance needs would improve industry-wide cyber security readiness and performance.

These conclusions are supported by research that demonstrates the significant and favorable influence of management support, resource considerations, and regulatory factors on SMEs' adoption of cyber-security.

The first goal of the study found that senior management support significantly enhances the cyber-security of SMEs in Mogadishu, influencing resource allocation and policy implementation. This suggests a strategy for managers to manage digital environments and ensure the security of small and medium-sized businesses. The study indicates that enhancing management support significantly enhances cyber security preparedness. by a factor of.547. According to Hsu et al. (2012) Senior management's involvement in information security management is crucial for successful adoption of information systems security, as commitment to cyber security is determined by adherence to security policies.

The second goal of the study found that resource variables significantly impact cyber security readiness among SMEs in Mogadishu, Somalia. Modifying resource parameters significantly increases preparedness by a factor of.045, focusing on the availability and allocation of resources. The study evaluates Mogadishu's SMEs' readiness to adopt comprehensive cyber securitymeasures, focusing on technical aspects. The results show that a strong IT infrastructure can boost preparedness for cyber-attacks, making IT infrastructure development crucial for organizational readiness. (Kong et al., 2012b)

The third goal of the study was to look at how regulatory issues in Mogadishu, Somalia influenced the city's degree of cyber security preparedness. The investigation revealed that regulatory considerations have a favorable and substantial impact on the cyber security of SMEs. Regulations can also help with cyber security. According to the report, businesses can create cyber-security frameworks using rules as tools. Companies with skilled leadership that invest in cyber-security technology and cyber- security training will be more competitive and capable of becoming cyber-aware. The study found that modifying regulatory parameters significantly enhances cyber security by a factor of 200. Regulations guide enterprises in achieving cyber-security byproviding legal and security frameworks, impacting preparedness and performance in SMEs, and influencing their cyber security architecture. Government aid is crucial for enhancing company cyber security, as per deterrence theory, and strengthening organizational readiness to combat cyber-attacks by expanding cyber security expertise. (Maow, 2021).

VII. CONCLUSIONS

The findings of the study demonstrate that the three primary factors of management support, resources, and regulatory considerations are essential for the implementation of cyber security preparedness in the Mogadishu Small and Medium-sized Enterprises (SMEs). This is in line with the fundamental principles of commitment to cyber security policies and standards that can be used to measure the level of cyber security commitment among top management. The human component is an important aspect of cyber security. Organizational security culture is influenced by changing user behavior, and staff training and awareness are crucial for cyber security preparedness, as individuals can be targets for social engineering. These Studies highlight the importance of organizational skills in managing cyber security in enterprises, suggesting that training, education, and awareness initiatives can enhance workers' abilities. (Mose, 2019).

Management support refers to the extent to which the top-level management of SMEs in Mogadishu, Somalia, prioritizes and actively participates in cyber security initiatives. This variable assesses how much importance and resources the management dedicates to promoting a strong cyber security culture within the organization. Management support plays a crucial role in determining the level of emphasis and priority given to Cyber security within an organization. Research has shown that SMEs with strong leadership commitment and support towards Cyber security tend to have higher levels of preparedness and better Cyber security performance. Additionally, managers can support cyber-security by offering training programs for their staff, encouraging staff to adopt new procedures, and reducing employee resistance to change. (Kemper, 2019)

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL264

Basically, resources are anything that an organization has access to, either physically or digitally, that they own, manage, or have semi-permanent control over. Resource factors are the building blocks of tech readiness, positivity, and innovation, whichis a great way to respond to new tech and give people the freedom, control, and efficiency they need to be early adopters and leaders in new tech. Technical Capacity: SMEs, like bigger enterprises, must have teams of IS specialists to manage risks and prepare for a data breach. Suitable Personnel, Long-term security is greatly influenced by the availability of technically skilled personnel and employee morale. While the current study concentrated on cyber-security, particularly in small and medium-sized businesses (SMEs), this investigation was cross-industry in nature. Financial capacity is a crucial aspect in defending against cyber security risks and enforcing cyber security in SMEs.

Regulation is another key aspect of cyber security preparation. It contributes to company continuity and the protection of critical information. Government regulations are essential drivers of secure e-business transactions and hence have an influenceon the cyber security architecture of businesses. Deterrence theory-based information security. Governments may play a varietyof roles and adopt a variety of actions to govern company cyber security. According to deterrence theory, government aid is critical in ensuring company cyber security, and governments may take a number of activities to enhance cyber-security (Maow, 2021).Governments, according to (Kenneth J. Knapp et al., 2006), must take responsibility for information security by implementing cyber security programs.

It is evident that a company's ability to achieve its organizational goals, particularly in the area of cyber security, is significantly influenced by the resources at its disposal. A company's capacity to withstand and recover from cyber-attacks is significantly influenced by its level of technological proficiency, managers' awareness and support for cyber-security preparation, and the pace of regulatory change. Managers can evaluate the ongoing defense strategies to be used and focus investments on the most efficient defense strategies as a result. They were also valuable in illustrating how firms respond to the cyber security environment by changing and adapting policies and procedures such as information sharing.

REFERENCES

[1]. AlEnezi, A. (2019). Internet of Things & Cybersecurity Readiness in Smart-government and Organizations. *Kuwait University*, *February 2020*, 1–55. https://doi.org/10.13140/RG.2.2.17160.34563

[2]. Angst, C. M., Block, E. S., Arcy, J. D., & Kelley, K. (2017). *R Esearch a Rticle W Hen D O It S Ecurity I Nvestments M Atter ? a Ccounting for the I Nfluence of I Nstitutional F Actors in the C Ontext of H Ealthcare D Ata B Reaches 1*. *41*(3), 893–916.

[3]. Assefa, T., & Tensaye, A. (2021). Factors influencing information security compliance: an institutional perspective.

[4]. *SINET: Ethiopian Journal of Science*, *44*(1), 108–118. https://doi.org/10.4314/SINET.V44I1.10

[5]. Bell, S. (2017). Cybersecurity is not just a “big business” issue - Governance directions : journal of Governance Institute of Australia Ltd. *Governance Directions : Journal of Governance Institute of Australia Ltd.*, *69*(9), 536–539.

[6]. Catota, F. E., Granger Morgan, M., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. *Journal of Cybersecurity*, *5*(1), 1–19. https://doi.org/10.1093/cybsec/tyz001

[7]. Chang, Y. W., & Chen, J. (2021). What motivates customers to shop in smart shops? The impacts of smart technology and technology readiness. *Journal of Retailing and Consumer Services*, *58*(May 2020), 102325. https://doi.org/10.1016/j.jretconser.2020.102325

[8]. CyberTalents. (n.d.). *What is Cyber Crime? Types, Examples, and Prevention - CyberTalents*.

[9]. D’Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems*, *31*(2), 285–318. https://doi.org/10.2753/MIS0742-1222310210

[10]. Daniel, D. (2015). No Title空間像再生型立体映像の研究動向. *Nhk技研*, *151*, 10–17.

[11]. Daud, M., Rasiah, R., George, M., Asirvatham, D., & Thangiah, G. (2018). Bridging the gap between organisational practices and cyber security compliance: Can cooperation promote compliance in organisations? *International Journal of Business and Society*, *19*(1), 161–180.

[12]. Gafni, R., & Pavel, T. (2019). The invisible hole of information on SMB’s cybersecurity. *Online Journal of Applied Knowledge Management*, *7*(1), 14–26. https://doi.org/10.36965/OJAKM.2019.7(1)14-26

[13]. Hsu, C., Lee, J. N., & Straub, D. W. (2012). Institutional influences on information systems security innovations.

[14]. *Information Systems Research*, *23*(3 PART 2), 918–939. https://doi.org/10.1287/isre.1110.0393

[15]. Kankanhalli, A., Teo, H. H., Tan, B. C. Y., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, *23*(2), 139–154. https://doi.org/10.1016/S0268- 4012(02)00105-6

[16]. Kemper, G. (2019). Improving employees’ cyber security awareness. *Computer Fraud & Security*, *2019*(8), 11–14. https://doi.org/10.1016/S1361-3723(19)30085-5

[17]. Knapp, K. J., Marshall, T. E., Rainer, R., & Ford, F. N. (2005). Managerial Dimensions in Information Security: A Theoretical Model of Organizational Effectiveness. *International Information Systems Security Certification Consortium (ISC)*, 2.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUL264

[18]. Kong, H. K., Kim, T. S., & Kim, J. (2012). An analysis on effects of information security investments: A BSC perspective. *Journal of Intelligent Manufacturing*, *23*(4), 941–953. https://doi.org/10.1007/S10845-010-0402-7/METRICS
Kumar,
[19]. S., Biswas, B., Bhatia, M. S., & Dora, M. (2020). Antecedents for enhanced level of cyber-security in organisations. *J. Enterp. Inf. Manag.*, *34*(6), 1597–1629. https://doi.org/10.1108/JEIM-06-2020-0240
[20]. Lloyd, G. (2020). The business benefits of cyber security for SMEs. *Computer Fraud and Security*, *2020*(2), 14–17. https://doi.org/10.1016/S1361-3723(20)30019-1
[21]. Mose, T. (2019). Factors influencing cybersecurity readiness in deposit taking savings and credit cooperatives : A case study of Nairobi county. *International Academic Journal of Information Systems and Technology*, *2*(1), 157–182.
[22]. Muriithi, S. (2017). *African Small and Medium Enterprises (Smes) Contributions, Challenges and Solutions*. *March*.
[23]. Neri, M., Niccolini, F., & Pugliese, R. (2022). Assessing SMEs' cybersecurity organizational readiness: Findings from an Italian survey. *Online Journal of Applied Knowledge Management*, *10*(2), 1–22. https://doi.org/10.36965/ojakm.2022.10(2)1-22
[24]. Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). *An introduction to information security*. https://doi.org/10.6028/NIST.SP.800-12R1
[25]. Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly: Management Information Systems*, *34*(4), 757–778. https://doi.org/10.2307/25750704
[26]. Ravichandran, T., & Rai, A. (2000). Quality management in systems development: An organizational system perspective. *MIS Quarterly: Management Information Systems*, *24*(3), 381–410. https://doi.org/10.2307/3250967
[27]. Rezaei, J., Ortt, R., & Trott, P. (2015). How SMEs can benefit from supply chain partnerships. *International Journal of Production Research*, *53*(5), 1527–1543. https://doi.org/10.1080/00207543.2014.952793
[28]. Techopedia. (2022). *What is Cyberspace? - Definition from Techopedia*. Techopedia.
[29]. Yliopisto, J. (2017). *MOTIVATIONS BEHIND EMPLOYEE INFORMATION SECURITY BEHAVIOR*.