ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN641

Organizational Factors that Influence Information Security in Smes: A Case Study of Mogadishu, Somalia

Hassan Adan Hussein
Computer Science & IT
Mogadishu University
Mogadishu, Somalia

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

Abstract:- Many organizations and businesses are currently dependent on information systems to conduct their business process and transactions. The security of the information being handled by systems has become a challenge in the corporate world today, as organizations strive to take measures to safeguard their information and maintain confidentiality. The study aimed to investigate the factors that influence information security in Small and medium-sized enterprises (SMEs) in Mogadishu Somalia. The study was guided by the following research objectives: such as organizational characteristics, data management practices, and employee characteristics in organizations that affect information security in SMEs in Mogadishu Somalia. A quantitative descriptive research design was used in this study, whereby the population consisted of 150 respondents which was focused on Owners, Managers, and Information Security Engineers of Small and Medium-sized enterprises (SMEs) in Mogadishu. Out of which a sample size of 140 respondents was obtained, spread out across three categories. The researchesr applied the probability method to select Owners, Managers, and Information Security Engineers from the Small and Medium Enterprises in Mogadishu Somalia. The elements selected from the population interacted with information security and were well-qualified to respond to the research objectives. The researches used self-administered structured questionnaires, whereby the respondents were required to point out the measure of appropriateness of the three main factors that influence information security in SMEs in Mogadishu. The questionnaire used a five-point Likert-type scale ranging from strongly disagree (1) to strongly agree (5). The respondents were also asked to indicate demographic information that comprised of Sex, age, level of education, years of experience, job position, and marital status, based on their perception and understanding. The study was a quantitative research design, whereby a total of one hundred and fifty (150) questionnaires were distributed and one hundred and fourty (140) were returned from the respondents, indicating a response rate of 99%. The analysis of the data was performed in a quantitative nature so as to obtain numerical data made use of descriptive and correlation statistics and was analyzed using SPSS software. The data was structured according to the research objectives and displayed in the form of tables.

Keywords:- *Information Security, SMEs Information Security, Mogadishu, Somalia.*

I. INTRODUCTION

In today's rapidly evolving digital landscape, information security has become a top concern for organizations worldwide, regardless of their size or industry. Small and Medium Enterprises (SMEs) in particular, play a vital role in driving economic growth and development in emerging markets like Mogadishu, Somalia. However, SMEs often face unique challenges in safeguarding their sensitive information and digital assets, as they may have limited resources and expertise compared to larger corporations.

This research aims to delve into the specific organizational factors that impact information security practices in SMEs operating within Mogadishu. By identifying and analyzing these factors, stakeholders, policymakers, and business owners can gain valuable insights into the challenges faced by SMEs and devise targeted strategies to enhance their cybersecurity measures. Small and medium-sized enterprises (SMEs) spanning various sectors in Mogadishu, from manufacturing and retail to service-oriented businesses. In this context, understanding the organizational factors that influence information security is crucial for SMEs to effectively protect their data, customer information, and business operations from potential cyber threats.

Academics predict a 30% increase in growth for organizations dealing with constantly expanding information amounts. (Chaffey, D. and Wood, S. (2005).

As information volume increases, organizations face challenges in managing and securing their information and making informed IT investment decisions to mitigate known and undiscovered risks. (Adomavicius et al., 2008b)

Organizations are prioritizing information security as it is an essential resource and a vital business component (McAdams, 2004).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN641

In this paper discusses and evaluates factors that influence an organization including organization characteristics, data management practices, and employee characteristics;

- **Organizational characteristics** enable private and public to achieve goals beyond individual capabilities, varying widely and evolving. Understanding these is crucial for effective management and strategic decision-making.
- **Data management** is the strategic use of data to enhance organizational performance by developing strategies, implementing systems, and enhancing information quality.
- **Employee's characteristics** significantly impact an organization's information security, making their actions crucial. Understanding employee characteristics and promoting awareness is key to effective security. Regular training, workshops, and simulations can help employees make responsible decisions and adhere to security protocols.

II. LITERATURE REVIEW

In this literature review, we will examine the various factors that affect information security in organizations in Mogadishu Somalia. The Paper is arranged on the base of the research questions. First will be the organizational characteristics that influence information security aspects and styles that play a role in information security SMEs in Mogadishu. The review will also have a look at some of the established standards and ways in which data is managed in small and medium enterprises (SMEs) and how it contributes to the organization's information security. The other objective will be to review how Information Security Engineers' attributes in organizations affect information security.

A. Organizational Factors that Influence Information Security in SMEs:

The research questions serve as the basis for organizing this chapter. Information security is influenced by organizational characteristics and styles, which will be discussed first. Next, certain recognized guidelines and practices for managing data in businesses will be examined, along with how they support information security within the company. Reviewing the impact of personnel characteristics on information security within firms will be the other goal.

B. Organizational Characteristics and Information Security

This study discusses the following Organizational Characteristics when securing the information assets of SMEs: Organizations are legal structures that enable public and private sectors to collaborate towards achieving or realizing goals that would not have been achievable by an individual.(James Gibson, John Ivancevich, 2011). Organizations have a strategy, outlining their purpose, goals, plans, and procedures, including mission, objectives, strategies, and policies, which are implemented differently. However, as (Hall & Griffin, 2012) Some basic elements that organizations use to implement their strategies include procedures, budgets, and programs.

Organizations prioritize security as a top priority, similar to prioritizing other services like excellent client services. They often have guidelines called policies, which help in problem-solving and decision-making. Policies provide specific information about an organization's security approach and are used as a control tool to reduce risk, address vulnerabilities, and respond to attacks. Implementing policies, along with awareness, technology, and education, supports information security, ensuring employees understand and value their responsibility to protect information technology systems and data. (Whitman et al., 2016)

Future technological advancements may alter the value of current technologies, making it challenging for businesses to invest effectively in information technology. Information security training focuses on improving employee performance and managing information systems, with IT professionals playing a critical role.(Bulgurcu et al., 2010) IT professionals require technical training and certifications to stay informed about security trends and threats. User familiarity with IT is crucial for IT governance practices. Employee adherence to security policies is influenced by training, and a non-punitive approach is more effective.(KIHARA, 2015)

Risk management and security involve controlling and mitigating loss from incidents, including intentional or accidental. Organizations should have a system in place to manage risks, especially with heavy reliance on information systems. (KIHARA, 2015),

Proper risk management is crucial for organizations to safeguard resources, provide a safe experience for employees, and continue operating. There are three main categories of risk management activities: risk identification, risk assessment, and risk control. Studies show that most cybercrime and information loss incidents go unnoticed, emphasizing the importance of risk management. However, there is a gap in research on business risk management in information security, leading to insufficient resources for security-related programs. Effective risk management requires both management and staff involvement in early threat detection and response. (Whitman & Mattord, 2011) Organizations are adopting secure systems like Authentication Services, Firewalls, and Antivirus Apps to protect their information in today's complex business environment.(Walkowski, 2019).

C. Data Management Practices and Information Security

This section enforces the following Data Management Practices, usage of information systems and backup recovery management. The rapid growth of data collection and storage in organizations necessitates effective data management and storage, as digital information is expected to grow by 1.2 zettabytes per year, according to I.T. executives. Information systems, often computer-driven,

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN641

consist of hardware, software, databases, and processes. Securing these systems is a top priority for organizations, as full security cannot be achieved overnight.

A business continuity management plan is crucial for organizations to address human error, natural disasters, state laws, and the nature of their business. Financial institutions and SMEs primarily use data storage and backup to comply with government regulations. Backup protects data from corruption, while a good policy reduces data loss risk. Data privacy is a crucial aspect of disaster recovery management, as stated by the European Commission. (KIHARA, 2015)

A business continuity plan (BCP) is a proactive, documented strategy for maintaining operations during and after disruptions or disasters, crucial for protecting resources and SMEs. Business continuity refers to an organization's ability to resume operations after a disaster, with minimal disruption to its systems and networks. It requires annual re-evaluation and testing to identify areas for improvement and ensure no gaps are missed.

D. Employee Characteristics and Information Security

This study discusses Information Tools and Resource Usage, Normative Beliefs, Employee Behavior in the Organization, and Policy Compliance Intention. Organizations use numerous IT tools and resources in their business processes, but it's crucial to assess their value and ROI. Telecommunications tools like instant messaging, email, internet, and mobile phones have transformed business operations. To avoid negative client and partner reviews and damage to reputation, organizations should focus on reducing IT asset abuse. (Adomavicius et al., 2008a)

The Internet has become a popular platform for people and organizations, with 70% of companies offering Internet access to over 50% of employees. The primary objective is to increase productivity through information, but misuse in the workplace is a major concern, according to a survey by Case and Young. (Liao et al., 2009), Puhakainen & Siponen's 2010 study highlights non-compliance with information security policies as a significant security failure in corporations. The attitude of employees towards compliance is influenced by their conformity, beliefs, and moral beliefs, making effective measures difficult to achieve.

James Gibson and John Ivancevich (2011) discuss the contentious topic of whether management can significantly change an employee's behavior, highlighting variables such as skills, demographics, experience, personality, and perception. Research indicates that employees' attitudes toward learning information systems are influenced by their psychological characteristics, including interest in IT, self-sufficiency, neutrality, retirement age, expectations, organizational roles, skills, health and safety, and project management utility. (KIHARA, 2015),

The frequency of implementing security measures depends on the frequency of their implementation, such as regular antivirus software updates, being cautious of suspicious emails, using strong passwords, and using firewalls. The intent to comply with security policies is influenced by user conduct, with self-efficacy being a key factor. Self-efficacy refers to an individual's belief in their ability to perform a task. (Straver & Ravesteyn, 2019).

The chapter is organized on the basis of the research questions. First shall be the organizational aspects and styles that play a role in information security. The review will then have a look at some of the established standards and ways in which data is managed in enterprises and how it contributes the organization’s information security. The other objective shall be to review on how employee attributes in organizations affect information security.

The text emphasizes the significance of clear and effective communication of information security policies for employee commitment, highlighting the potential negative impact of lack of knowledge on compliance and organizational security. This study focuses on the information security of organizations, assesses the relevance of factors affecting information security identified from previous studies, and investigates the impact of information security on three aspects of organizational performance

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN641

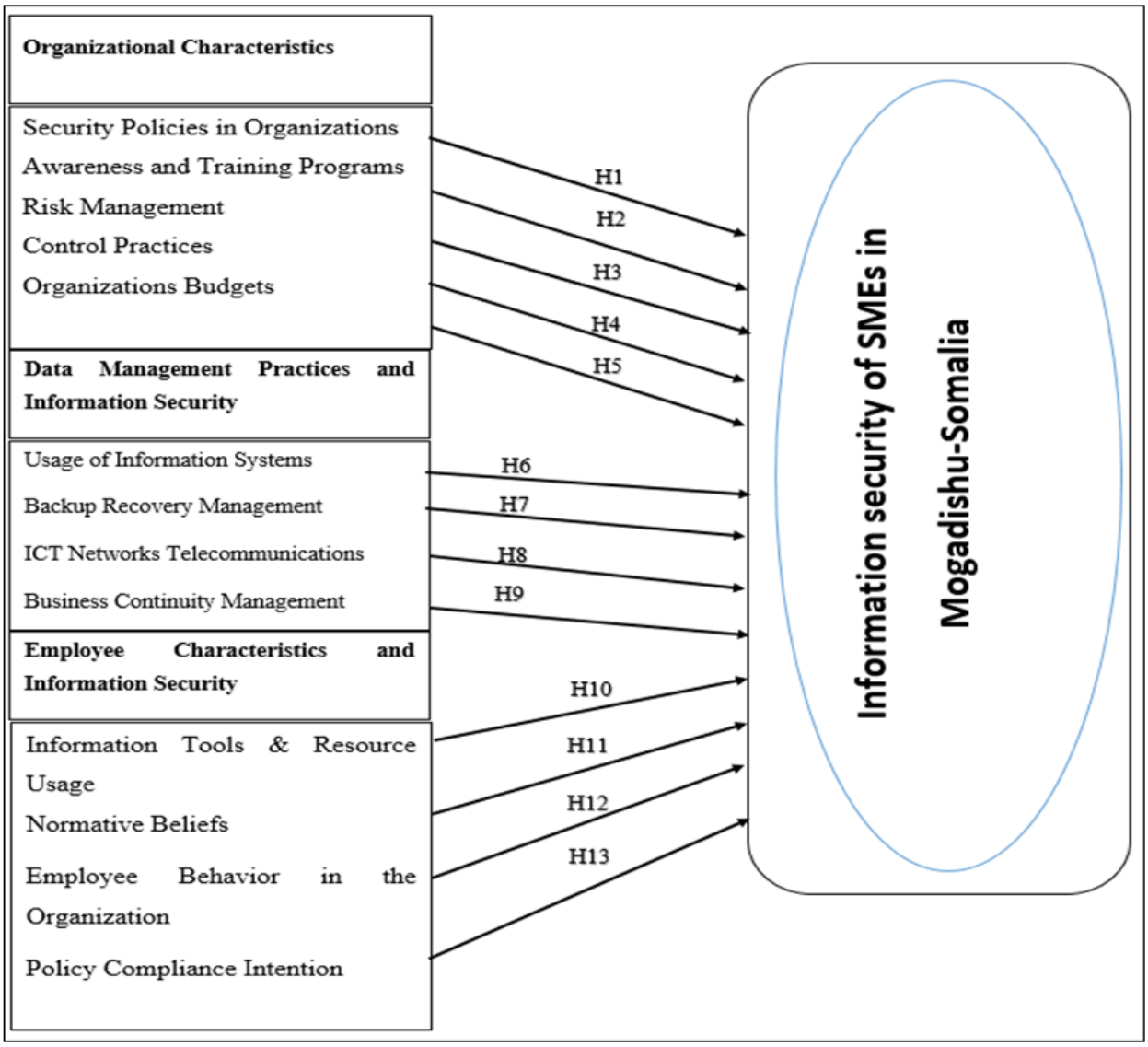

Fig.1. Information Security Model

E. Research Model and Hypotheses

Based on the thirteen components and environmental settings of the TOE framework, we develop an information security model (Fig. 1). The three theories are combined in this study inside the comprehensive TOE framework to provide a more complete understanding of the factors impacting companies' information security, notwithstanding their unique constraints.

This research uses the technical framework of the TOE framework to examine how Organizational Characteristics affect an organization's information security. The TOE framework's Data Management Practices and Information Security section also applies institutional theory to examine how organizational culture, backup recovery management, and information system usage impact an organization's information security. Theory is employed in the internal Employee Characteristics and Information Security of the TOE framework to comprehend how supplier/partner relationships and competitor collaboration affect an organization's information security.

Organizations empower the public to achieve objectives that an individual could not achieve. They have a strategy outlining their mission, objectives, strategies, and policies. Organizations implement their strategies differently, but basic elements like procedures, budgets, and programs help them achieve their goals.

H1. Organizations are defined as legal structures that enable the public and private to work toward achieving or realizing goals that could not have been reached by an individual

H2. Awareness and training programs are initiatives within organizations to educate employees on important topics like cybersecurity, diversity, workplace safety, compliance regulations, and company policies.

H3. Risk management and security refer to the management and mitigation of potential losses an organization may experience due to intentional or accidental incidents.

H4. Control practices in organizational management involve systematic methods, procedures, policies, and guidelines to ensure efficient operations, mitigate risks, safeguard assets, and promote compliance with internal and external regulations.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN641

H5. An organizational budget is a financial plan outlining an organization's projected revenues, expenses, and goals for a fiscal year, guiding resource allocation and financial decision-making.

Data management practices and information security are crucial components of organizational governance aimed at safeguarding sensitive information, ensuring data integrity, and managing data assets effectively.

H6. Information systems involve the use of various technologies, tools, and processes to collect, store, process, analyze, and disseminate data and information to achieve various objectives.

H7. Backup and recovery management is a crucial process for organizations to protect their data and ensure its availability in case of data loss, corruption, or system failures.

H8. ICT networks refer to the infrastructure and technologies used for data, voice, and multimedia transmission over networks, enabling connectivity and information exchange among devices and users.

H9. Business Continuity Management (BCM) is a comprehensive strategy for organizations to ensure critical business functions can continue or be swiftly restored in the event of disruptions or disasters.

Employee Characteristics and Information Security" refers to the intersection between the attributes, behaviors, and roles of employees within an organization and the measures implemented to safeguard sensitive information and data assets. This concept recognizes that employees play a significant role in ensuring information security and that their characteristics, behaviors, and access levels can impact the overall security posture of the organization.

H10. Information Tools & Resource Usage refers to the efficient use of various tools, technologies, and resources in personal and professional contexts to access, manage, process, and utilize information effectively.

H11. Normative beliefs are individual perceptions of socially acceptable behavior within a group or society, influencing attitudes, values, and behavior by providing standards for certain situations.

H12. Employee behavior in an organization encompasses actions, attitudes, and conduct in the workplace, including interactions with colleagues, supervisors, clients, stakeholders, task approaches, conflict handling, and adherence to organizational policies.

H13. Policy compliance intention refers to an individual's willingness to comply with organizational policies, rules, regulations, and guidelines, reflecting their intention to adhere to established procedures within the organization.

III. METHODOLOGY

Our study examines the organizational factors that influence information security in SMEs of Mogadishu, Somalia at the organizational level by focusing on different organizational aspects. A quantitative approach is adopted to investigate Information Security 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.

A. Target Population

Selecting for sampling proves to be a more advantageous approach compared to conducting a census, particularly in situations where urgency is a factor in obtaining research outcomes after data collection. The sample size is defined as several respondents that represent the population. Purposive sampling, a technique utilized in qualitative research, entails the deliberate selection of a specific subset of individuals or units for analysis. Unlike random selection, participants are chosen with intent, yielding alternative names such as judgmental sampling or selective sampling. In the context of purposive sampling, the researchers has a distinct objective in mind while selecting the sample. This approach involves choosing the sample based on specific attributes or characteristics of interest to the researchers. This method is most commonly applied in studies employing surveys.

This sample will be conducted on 10 SMEs in Mogadishu Somalia. The size of the sample can have a significant effect on the data collection methods and also the cost of conducting the entire research. Therefore, it is important to pay attention to the size of the sample to ensure the validity of the research. The size of the sample is determined by the Yamane's formula (Adam, 2020). 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 150 but 140 responded to the questionnaire and the focus of the study was Owners, Managers, as well as other Information Security Engineers within SMEs in Mogadishu, Somalia.

B. Questionnaire Procedures

The pilot study is designed to evaluate the relevance of the questionnaires to the study as well as to evaluate the precision of the questionnaires. The goal of the pilot study is to ensure that the questions are clear and straightforward in a way that the respondents can understand. Pilot testing allows the researcher to understand the relevance of the questions as well as the robustness of the collected data. A total of 10 questionnaires are sent to management, IT professionals, and employees in small and medium-sized enterprises (SMEs) in Mogadishu Somalia to assess the strength and completeness of the questionnaires. The questionnaires are then altered into useful results according to the recommendations from the 10 respondents. Each questionnaire is accompanied by a cover letter outlining the purpose of the study. After completing the survey, the researchers carried out a follow-up to gently remind respondents to complete the questionnaires.

C. Questionnaire Development

The survey method was used to complement the case study research in terms of getting the possibility of generalization. A survey is conducted about 10 SMEs in Mogadishu Somalia. A comprehensive questionnaire designed to cover the Information security of SMEs, the

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN641

current state of SMEs in Somalia, proposing information security in the Somali SMEs. Studying factors that influence SMEs, the study adapted the questionnaire of those sources and references shown in table 1.

Table 1 Categories of the Questionnaire.

Question. Constructors/ factors	Number of sub-Questions	Factors source/Reference
Demographic and SME information	6	Researchers
Organizational Characteristics	15	KIHARA, P. K. (2015).
Data Management Practices	12	Chaffey and Wood (2005),
Employee Characteristics	12	(Burchell, 2011a).

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, Organizational Characteristics, Data Management Practices, Employee Characteristics, and Information Security. Before starting the survey data collection process, the survey items were pre-tested in a pilot study of 10 SMEs 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.

D. Quality Assurance of the Research:

Quantitative data is collected. The first step will be to code the questionnaires based on the variables in the study. Then, the data will be inputted into a data analysis application: statistical package for the social sciences (SPSS), and descriptive statistics are performed on it describes descriptive statistics as techniques that "translate large sets of observations into a concise form that is easy to summary." The data is presented in tables and figures. The researchers used percentages to look at the Demographics, Organizational attributes, Data management practices, and Employee characteristics, and how they affected information security. This allows the researchers to gather relevant information that helps him to draw conclusions and recommendations.

IV. DATA ANALYSIS OF DEMOGRAPHIC CHARACTERISTICS

A. Data Analysis of Demographic Characteristics

The researchers demonstrated here the following demographic information: The respondent's gender, age, education, marital status, and 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 descriptive statistics such as 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 92. 1%. 7.9 % of the respondents were female that question is depicted in Table 2.

Table 2 Gender of the Respondents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	129	92.1	92.1	92.1
	Female	11	7.9	7.9	100.0
	Total	140	100.0	100.0	

➢ *Group of the Respondent Age*

In terms of the age of the respondents, the majority of the respondents were in the range 28 – 32 years old and accounted for 31.4 % whereby 21.4 % of the respondents were in the range 24 - 28 and 17.1% were in the range 32-36 and 12.1% of the respondents were 36 and 40 and 9.3% of the respondents were 41 and above and 8.6% were 24 and less as depicted in Table 3.

Table 3 The Group of the Respondent's Age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	24 and less	12	8.6	8.6	8.6
	24 - 28	30	21.4	21.4	30.0
	28-32	44	31.4	31.4	61.4
	32-36	24	17.1	17.1	78.6
	36-40	17	12.1	12.1	90.7
	41 and above	13	9.3	9.3	100.0
	Total	140	100.0	100.0	

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN641

➢ *The Education Level of the Respondent*

In terms of the education level of the respondents, the majority of the respondents hold a Master degree and accounted for 55.7 % whereas 41.4% of the respondents hold a bachelor degree.1.4 % of the respondents hold a diploma, and, 0.7 % of the respondents were PhD and secondary as depicted in Table 4.

Table 4 The Education Level of the Respondents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Secondary	1	.7	.7	.7
	Diploma	2	1.4	1.4	2.1
	Bachelor	58	41.4	41.4	43.6
	Master	78	55.7	55.7	99.3
	PhD	1	.7	.7	100.0
	Total	140	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 5-10 years and accounted for 37.9 % whereas 26.4 % of the respondents have less than 5 years in their experience and 17.1 % of the respondents have 10-15 years experience and 15.0 % of the respondents have 15-20 years of experience and 3.6 % have 20 years and above experience as depicted in Table 5

Table 5 The Years of Experience of the Respondents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less than 5 years	37	26.4	26.4	26.4
	5-10	53	37.9	37.9	64.3
	10-15	24	17.1	17.1	81.4
	15-20	21	15.0	15.0	96.4
	20 and above	5	3.6	3.6	100.0
	Total	140	100.0	100.0	

➢ *The Job Position of the Respondent*

In terms of job position of respondents, the majority of the respondents were Information Security Engineers and accounted for 57.1 % whereby 29.3% of the respondents were Managers and 13.6% of the respondents were Owners as depicted in Table 6.

Table 6 the Job Position of the Respondent

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Owner	19	13.6	13.6	13.6
	Manager	41	29.3	29.3	42.9
	Information Security Engineers	80	57.1	57.1	100.0
	Total	140	100.0	100.0	

➢ *Marital Status of the Respondents*

In terms of the marital status of the respondents, the majority of the respondents were married and accounted for 68.6 % whereas 31.4 % of the respondents were single as depicted in Table 7.

Table 7 the Marital Status of the Respondent

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Single	44	31.4	31.4	31.4
	Married	96	68.6	68.6	100.0
	Total	140	100.0	100.0	

V. CORRELATION ANALYSIS

The study focused on analyzing the effect of Organizational Characteristics, Data Management Practices, and Employee Characteristics on the Information security of SMEs in Mogadishu-Somalia. The research utilized the Pearson correlation coefficient approach and matrix as shown below.

The first objective analyzed the effect of organizational characteristics on the information security of SEs in Mogadishu-Somalia. This correlation indicates a weak positive relationship between “Information Security in SMEs in Mogadishu" and "Organizational Characteristics." However, this correlation is not statistically significant at the 0.05 level (2-tailed) since the p-value (Sig. (2-tailed)) is greater than 0.05 (specifically, it's 0.483).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN641

The second objective analyzed the effect of data management practices on the Information security of SMEs in Mogadishu-Somalia. This correlation indicates a weak positive relationship between "Factors Influencing Information Security in SMEs in Mogadishu" and "Data Management Practices." However, this correlation is not statistically significant at the 0.05 level (2-tailed) since the p-value (Sig. (2-tailed)) is greater than 0.05 (specifically, it's 0.264).

The third objective analyzed the effect of data management practices on the Information security of SMEs in Mogadishu-Somalia. This correlation indicates a very weak positive relationship between "Factors Influencing Information Security in SMEs in Mogadishu" and "Employee Characteristics." Additionally, this correlation is not statistically significant at the 0.05 level (2-tailed) since the p-value (Sig. (2-tailed)) is greater than 0.05 (specifically, it's 0.819).

In summary, based on this data, there are weak and non-significant correlations between "Factors Influencing Information Security of SMEs in Mogadishu" and each of the three variables: "Organizational Characteristics," "Employee Characteristics," and "Data Management Practices." The correlation matrix table below show the relation among the factors influencing Information Security of SMEs in Mogadishu Somalia.

Table 8 Correlation Matrix

		Factors influencing information SMEs in Mogadishu	**Orgazational Charactristics**	**Employee Characteristics**	**Data Management Practices**
Factors influencing information SMEs in Mogadishu	Pearson Correlation	1	.060	.020	.095
	Sig. (2-tailed)		.483	.819	.264
	N	140	140	140	140
Orgazational charactristics	Pearson Correlation	.060	1	.478**	.628**
	Sig. (2-tailed)	.483		.000	.000
	N	140	140	140	140
Employee characteristics	Pearson Correlation	.020	.478**	1	.484**
	Sig. (2-tailed)	.819	.000		.000
	N	140	140	140	140
Datamanagement practices	Pearson Correlation	.095	.628**	.484**	1
	Sig. (2-tailed)	.264	.000	.000	
	N	140	140	140	140

**. Correlation is significant at the 0.01 level (2-tailed).

VI. DISCUSSION OF THE FINDINGS

This section provides the results and findings of the study about investigating factors that influence the information security of SMEs in Mogadishu. The study looked at the key issues observed amongst the owners, managers, and employees at Mogadishu SMEs, concerning organizational characteristics, data management practices, and employee behavior. In addition, the study highlighted the problems in the existing research and also gave areas for further research. the first goal of the study found that Organizational Characteristics and Information Security are dealing with massive amounts of information that are constantly expanding. According to academics' estimates, growth is expected to increase by 30%.(Chaffey, D. and Wood, S. (2005). The challenges of managing such information increase as the amount of information increases. Organizations are attempting to make the best IT investment decisions to manage and secure their information from both known and unknown risks while the information technology (IT) market is also continually growing. (Adomavicius et al., 2008b) Organizations are starting to prioritize the security of their information since it is an essential resource, and security has become a vital component of business. (McAdams, 2004) therefore.

The initial goal was to determine the impact of Organizational Characteristics on Information Security in SMEs in Mogadishu. According to the findings, Organizational Characteristics have a considerable favorable influence on the information on firms. According to the study, improving organizational characteristics considerably improves information security preparedness.

The second goal of the study found that Data Management Practices and Information Security.

Is the process of managing data as a strategic resource for improving organizational performance and its information security This process involves developing strategies and introducing systems and information security controls to improve information quality to deliver value(Chaffey, D. and Wood, S. (2005).

The study's goal was to establish the link between Data Management Practices and Information Security According to the findings, Data Management variables have a substantial impact on Information Security in SMEs in Mogadishu Somalia. This is because a company's data management is the level of investment and implementation of data management measures inside the organization. The

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN641

study discovered that protection data parameters considerably increase information security preparedness.

The third goal of the study found that Employee Characteristics and Information Security.

Investigating on employee characteristics that could influence information security, one of them being information tools and resource usage the third goal of the research was to look at the impact of employee characteristics variables on Information Security in SMEs in Mogadishu, Somalia. The investigation revealed that employee characteristics considerations have a favorable and substantial impact on the information security of SMEs. Employee characteristics can also help with information security. The report cites employees as tools that businesses may use to establish information security frameworks. Firms with competent management that invest in information security technology and trained cyber security will be more competitive and capable of becoming information security aware.

VII. CONCLUSIONS

Organizational characteristics were found to be highly significant in the influence it has towards information security at SMEs Mogadishu. Hence it can be concluded in this study that organizational characteristics influence information security in Small and Medium-sized enterprises in Mogadishu. This therefore confirms that organizational characteristics are a critical factor in achieving information security in SMES Mogadishu Somalia.

The study established that the awareness, implementation, and management of information security policies have a strong influence on information security. This implies that SMEs should ensure that proper information security policies have been developed, implemented, and updated regularly.

Data management practices were found to be highly significant in the influence it has on information security at SMEs in Mogadishu. Hence it can be concluded in this study that data management practices influence information security in SMEs in Mogadishu. This therefore confirms the status of this factor as a critical factor in achieving information security in SMEs. Data management was observed to be a key factor amongst respondents in their view of data backup and recovery practices. The study revealed that proper implementation of backup and recovery procedures is a key contributor towards achieving information security.

More findings on data management practices drew the conclusion that the ICT department plays a major role in helping employees understand and properly utilize the various information systems set in place. That will ensure that the employees are equipped with the necessary skills required to handle the organization's information and therefore ensure of its security.

Employee characteristics were found to be highly significant in the influence it has on information security. Hence it can be concluded in this study that employee characteristics influence information security in SMEs. This therefore confirms the status of this factor as a critical factor towards achieving information security in SMEs in Mogadishu.

Employee characteristics were indicated as highly important amongst respondents in view of their attitudes and willingness to comply with the set information security policies. The findings revealed that their actions are highly influenced by their normative beliefs and self-efficacy or the belief that an individual carries the ability to undertake a particular activity. Therefore, management should make an effort to convince employees that full compliance with information security policies is indeed achievable.

REFERENCES

[1]. Adomavicius, G., Bockstedt, J. C., Gupta, A., & Kauffman, R. J. (2008a). Making sense of technology trends in the information technology landscape: A design science approach. MIS Quarterly: Management Information Systems, 32(4), 779–809. https://doi.org/10.2307/25148872

[2]. Adomavicius, G., Bockstedt, J., Gupta, A., & Kauffman, R. J. (2008b). Understanding evolution in technology ecosystems. Communications of the ACM, 51(10), 117–122. https://doi.org/10.1145/1400181.1400207

[3]. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Qjarterly Special Issue Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness1. Source: MIS Quarterly, 34(3), 39.

[4]. Chaffey, D. and Wood, S. (2005) Business Information Management Improving Performance Using Information. Pearson Education Ltd., Upper Saddle River. - References - Scientific Research Publishing. (n.d.). Retrieved July 19, 2023, from https://www.scirp.org/(S(351jmbntvnsjt1aadkposzje))/reference/ReferencesPapers.aspx?ReferenceID=1392681

[5]. Hall, P., & Griffin, J. J. (2012). Book Review - Wheelen and Hunger ' s Strategic Management and Business Policy : Toward Global Sustainability , 13 th. 419–422.

[6]. James Gibson, John Ivancevich, R. K. (2011). Organizations: Behavior, Structure, Processes. 640. https://books.google.com/books/about/Organizations_Behavior_Structure_Process.html?id=0ExYcgAACAAJ

[7]. KIHARA, P. K. (2015). Organizational Factors That Influence Information Security in State Corporations : a Case Study of Kenya National Highways Authority By.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN641

[8]. Liao, Q., Gurung, A., Luo, X. I. N., & Long, L. I. (2009). Workplace management and employee misuse: Does punishment matter? Journal of Computer Information Systems, 50(2), 49–59.
[9]. McAdams, A. C. (2004). Security and risk management: a fundamental business issue: all organizations must focus on the management issues of security, including organizational structures, skill sets, processes, and methodologies for managing security and risk management. Information Management Journal, 38(4), 36–42. http://www.freepatentsonline.com/article/Information-Management-Journal/119570070.html
[10]. Straver, P., & Ravesteyn, P. (2019). End-user Compliance to the Information Security Policy: A Comparison of Motivational Factors. Communications of the IIMA, 16(4). https://doi.org/10.58729/1941-6687.1396
[11]. Walkowski, D. (2019). What Are Security Controls? F5 Labs. https://www.f5.com/labs/learning-center/what-are-security-controls
[12]. Whitman, M. E., & Mattord, H. J. (2011). Principles of Information Security Fourth Edition. Learning, 269, 289.
[13]. Whitman, M. E., Mattord, H. J., Mackey, D. H., Green, A., TIPTON, H. F., Muscat, I., Clark, P. G., Agah, A., Chanda, K., Carlson, J., & Calder, S. R. (2016). Guide to Network Security. Security Intellegence: Analysis and Insight for Information Security Professionals, 2(7), 361. https://books.google.com/books/about/Guide_to_Network_Security.html?id=jML6CAAAQBAJ