RESEARCH ARTICLE OPEN ACCESS

Managing Information Security in Small and Medium Enterprise in East Africa

[1] MASESE CHUMA BENARD
Ass-Lecturer, Kampala International University-Western Campus, Department of Computing
[2] NGULENI FAITH,
Department Of Computer Science/Ict – Ass-Lecturer Tanzania Public Service College
[3] MASOUD CHARLES,
[4] MANYANGE NYASIMI MICHEAL,
Lecture, Kampala International University--Western Campus, School of Business And Management
[5] EDWIN WASIKE SIMITI,

ABSTRACT
Cybercrimes poses a great threat to the information security in small and medium enterprises, even technologically developed countries they face they also are also not left behind; it is important to understand the different types of crimes that affect the small and medium enterprises. Information security user demeanor is seemly growing attacks to their enterprise information security. The research used two objectives that is to assess the information security issues experienced in small and medium enterprise in east Africa, to examine the current security measures used by the sme's small and medium enterprise in east Africa. This paper used the descriptive survey; with 48 respondents the questionnaires were employed to collect primary data from the field. The finds show that it shows that 29.2% strongly agree that there is loss of data while on transit, 31.3% agree, that amount to 60.4% who strongly and agree. While 20.8% are neutral,14.6 disagree, strongly disagree 4.2%, Risk of unauthorized access by insiders and outsiders with a mean of 2.3958 and a standard deviation of 1.066670 implies that most respondents strongly agree that data is being corrupted with virus. Risk of deliberate act of information access and use with a mean of 2.3542 and a standard deviation of 1.02084. the conclusion, Confidentiality and privacy concerns were identified as an associated concern with security issues in sme's. Encryption is suggested as a better solution to secure information. Before storing data in cloud server and other storage devices, it is better to encrypt data. Data Owner can give permission to particular group member such that data can be easily accessed by them.

INTRODUCTION

The safeguarding of information and information systems from prospective non-authorized access, usage, disclosure, disruption, tempering, perusing, review, record or destruction is called information security. Therefore, information security is a crucial field in our society today. Information security is determined by the user who; access the systems and use the technologies that enable these tasks in accordance with which it takes place (Erceg, 2019; Surwade & Patil, 2019). Emerging trends in information security need to include people in ensuring information security of an enterprise (Woretaw, Lessa, & Negash, 2019). Bearing in mind that Security can be defines as "The status or quality of being secure that is to be at liberty from endangerment." It means to be secure against risks and from those individuals who would do harm, accidental or intentionally (Surwade & Patil, 2019).
Nowadays Information security is most significant and paramount topic influencing the performance banking sector and sme's. With the availability and use of information technology and raising level of networking to the global environment, sme's are prone to widespread of risks and threats (Woretaw, Lessa, & Negash, 2019). The goal of information security metrics is to detect or prevention of unauthorized access and use of information technology. Employees and people constitute social and organizational issues of Information security because experts must operate and use the information systems (Aleksandar, 2019). Information security is often considered to consist of confidentiality, integrity, availability, and accountability (Chen, 2009).

Information systems is comprised a collections of computing devices for example (hardware, programs, and firmware), procedures, and people, coupled jointly to dispense the enterprises with the capableness to process, store, and communicate information in a well-timed manner to keep up various missions and business functions. Information availability, accuracy and integrity enable a company to make good and modern business decisions (Amarachi, Okolie, & Ajaegbu, 2013).

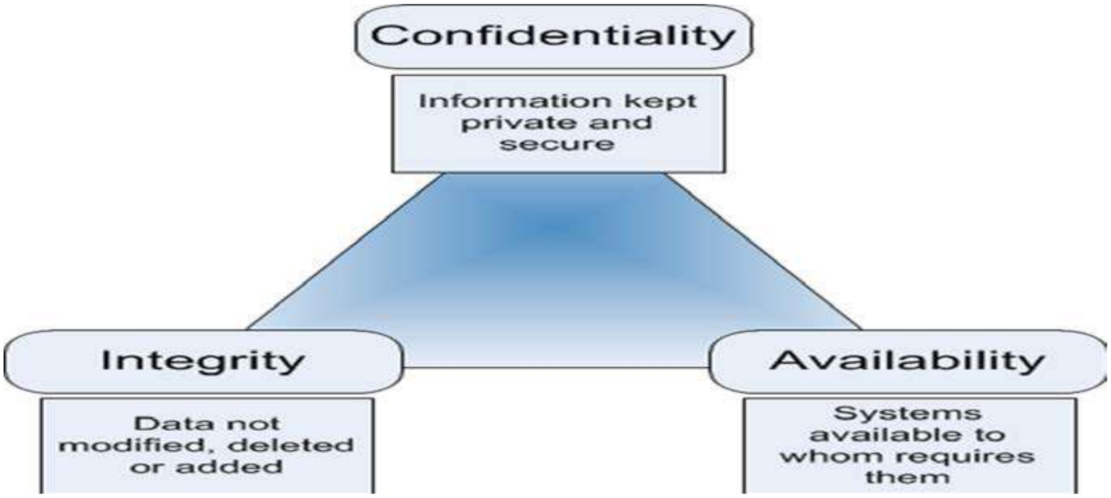
GOALS OF SECURITY

1. Non-Repudiation: the concept of non-repudiation is when the transmitter of the information cannot reject or rebuff the fact that he/she never transmitted the information. This rationale adopts digital signatures to avoid the transmitter from refusing being the source of the information (Gençoğlu, 2019). Ensure the user does not refuse that he/she used the information system (Alhassana & Adjei-Quaye, 2017).

2. Confidentiality –the information should be treated as private. Information shall be transferred to people on the access list for example to protect the information from reaching, access and use to unauthorized parties (Abbas, Mahmood, & Hussain, 2015). Information in the information system remains private to trusted parties or users (Alhassana & Adjei-Quaye, 2017).

3. Authentication – authentication is the most significant concept of cryptography for identifying the origin of the information. When the origin of information is recognized, it is easy to transmit it securely. Authentication is can adopt symmetric and asymmetric keys exchange to be used by the send and the receiver to prove identity and access (Tuncay, 2019).

4. Integrity – keeping with the exactness and totality of the information collection over its development stages that comprise to supervise and scrutinizing tampering to the information and information systems (Laybats & Tredinnick, 2016). Ensure the message has not been modified in network and is secured during transmission time. (Alhassana & Adjei-Quaye, 2017)


Confidentiality
Information kept private and secure
Integrity
Data not modified, deleted or added
Availability
Systems available to whom requires them

CIA architecture Adopted from (Alhassana & Adjei-Quaye, 2017)

The security triad comprises of three concepts that is, confidentiality, integrity and availability, integrity is the virtually crucial to manage operations. The authentication of exploiter and the coherent delivery of the appropriate information are constant important. Whereas confidentiality of the information may be required, it is not a relentless driver. Accessibility of security management applications has gained some interest because most applications can remain to process and maintain status information throughout disruption in communications. It may come along with security management system that supervises the trustworthiness of applications that should go through the same operose testing and analysis as the main security application (Singh, 2017).

The most critical job is to achieve a “state of security” is not obtaining the necessary tools, but selecting and integrating the right security metrics to provide an inclusive and authentic chain of security (Singh, 2017).

The problem identified in the SMEs is they invest limited capital and recruit less skilled manpower in setting up and nurture information technology security guidelines and plan of action. This inadequacy of information security cognizance and absence of right information security guidelines by SMEs lend them vulnerable to attacks, denial of service, threats, malicious codes and cyber-terrorists. In spite of the challenges and attacks facing the SMEs, their adoption, dependence and use on information communication and technology is significantly growing, and the enterprises objectives are directly being linked up with the use of information communication and technology (Abbas, Mahmood, & Hussain, 2015).

STATEMENT OF THE PROBLEM

Information security for an organization is becoming a paramount issue in the in the current information era. Approach to information, information systems and information security is an issue of great concern where user awareness and behavior plays a critical part. Information security user demeanor is seemly growing attacks to their enterprise information security. Information security's main objective's undertakings is detecting and preventing of unauthorized information technology access, use, modification, destruction and recording. Information security is a social and corporate problem because technical systems must be handled and used by people. Information and communication technologies users play a critical role in the information system security (Erceg, 2019). Sme's have limited resources to dedicate to information security hence managing information security among the enterprises is a critical subject in the globe today.

OBJECTIVES

1. To assess the information security issues experienced in small and medium enterprise in east Africa.
2. To examine the current security measures used by the sme's small and medium enterprise in east Africa.

LITERATURE REVIEW

According (Aleksandar, 2019) Information security includes users and technology. Approximately 90% of society and enterprises encounter at least one information security problems during the business year. Information security constitutes the guarding of information systems and data from potential non-authorized accessing, using, and disclosure, disruption, tampering, perusing, inspecting, recording or destructing. Information security is an important topic in our society. Information security is determined by the users who access and use the computing devices and technologies that enhance the business processes.

According to (Zhi & Atif Ahmad, 2013) they noted that SMEs are not dedicating resources towards information security. Because they have developed a sense that some information security implementations will have an effect on the efficiency of business operations. Information security is crucial, sme's endeavor to strike a balance between upholding right security guidelines and not having lasting impact the line of operation, also reassert that because the sme's are growing enterprises, too many layers of a system security may be a limitation to the operation and management of the information security.

The security layers an enterprise must adopt to implement security and protection of its activities and information assets. **Physical Security:** To safe guard the physical devices, objects, or areas of an company from non-authorized, users, accessing and misuse. **Personal Security:** the act of protecting the people or group of people who are permitted to access the enterprise and its cognitive process. **Operations Security:** Protecting the inside information of a specific cognitive process or a number of processes. **Communications Security:** Protecting an enterprise's communications media, technology, and content. **Network Security**: securing networking components, connections, and contents stored in the databases or on transmissions. **Information Security:** Guarding of information and its significant elements, involving the systems and hardware from authorized access, use and transmit (Surwade & Patil, 2019).

The great percentages of the actual information security vulnerable areas in any organizations or tasks are not technological vulnerabilities but human beings or users of the system. Users have a habit of behaving in unpredictable and sometimes inexplicable ways. Hackers maximize the weakness of users to poses threats to information security. In some cases, they may adopt social engineering where it is the activity of engineering an individual to disclose passwords, access details or private information often by masquerading as an individual who is authorized to access the system (Laybats & Tredinnick, 2016).

Users of Information and communication technologies have a great impact information system security and are still termed as the weakest spot of information security (Aleksandar, 2019) . Technology adapted to information introduces a number of risks therefore information security is important. In some circumstances when information security risk is observed, it is important to create an information security policy. These policies are classified into four categories: protection measures, detection measures, consequences response measures and measures to ensure the effectiveness of the consequences response (Aleksandar, 2019).

According to (Surwade & Patil, 2019) in this Information era, Information is available everyplace. Knowledge is so significant for every organization's decision-making process. New security challenges are emerging day in day out from malicious codes that can be executed in user's personal computer, to phishing to gain access or deceive user into giving up private information, to malicious code like virus, worm (Surwade & Patil, 2019).

Threats to information security

Malware	**Vulnerabilities**	**Attacks**
Trojan	-Device –hardware	-Hardware based
Virus	-Software	-Device based
Worms	-people	-Software based
Spyware		- User based

The use of internet has facilitated the global reach to SME, networking the whole globe and has given them a platform to compete with the large and established enterprises on the equal level. But also, the internet poses a number of dangers and internet-based attacks. Defense against network-based threats and attacks require right expertise and training to overcome targeted threats, SMEs are more vulnerable to these attacks as cybercriminals have knowledge that SMEs invest little to security technology as compared to established organizations. Proper information security technology like firewalls, anti-virus, anti-malware, phishing filters shall be installed by the SMEs to reduce the internet-based threats (Abbas, Mahmood, & Hussain, 2015).

METHODOLOGY

Research design

This paper used the descriptive survey; the questionnaires were employed to collect primary data from the field. The representative sample was taken from the sme's from east Africa's business hub cities. To capture the responses of these individuals, a structured questionnaire was prepared, which was aimed to be administered to this entire selected population.

Sample size

The exercise produced a response of 48 completed questionnaires. Which were collected using google forms.

Table 1: **Sample of sme's from Nairobi, Kampala and Dar es salaam**

location of your business enterprise

	Frequency	Percent	Valid Percent	Cumulative Percent
Kenya	16	33.3	33.3	33.3
Uganda	16	33.3	33.3	66.7
Tanzania	16	33.3	33.3	100.0
Total	48	100.0	100.0	

Source: field data (2021)

The sample was selected from the three east African countries that is Kenya, Uganda and Tanzania respectively with equal sample size. The sample was taken from commercial hubs in those countries name Nairobi, Kampala and Dar es salaam cities.

Data Collection Method

Primary data collections and Secondary data collection

Primary data were used to collect data, structured questionnaires were developed and circulated through google form. The data are collected from sme's in east Africa business hub cities. The secondary data was done by using of journals, books, office reports, brochures and government documents and library on the literature review.

Sampling procedure

Simple random sampling was used in sampling the sme's in East Africa. The aim of using simple random sample was to reduce the potential for human bias in the selection of cases to be included in the sample. As a result, the simple random sample provided us with a sample that was highly representative of the population being studied, assuming that there is limited missing data. Since the units selected for inclusion in the sample are chosen using probabilistic methods, simple random sampling allows us to make generalizations *(i.e.* statistical inferences*)* from the sample to the population. This is a major advantage because such generalizations are more likely to be considered to have external validity.

DATA ANALYSIS AND RELIABILITY OF THE INSTRUMENT

The questionnaire were close-ended questions, using the likent scale of 1.0 strongly agree, 2.0 agree, 3.0 neutral, 4.0 disagree, 5.0 strongly disagree. Face validity of the questionnaire was performed to ensure the relevance of content and interpretation by discussing with experienced faculty members and researchers.

SPSSv20.0 software was used to generate descriptive statistics. Cronbach's Alpha was used to test the internal reliability of the questionnaire and it produced a result of 0.827, which show that the instrument used was reliable.

Reliability Statistics

Cronbach's Alpha	N of Items
.827	48

Data analysis

The questionnaire were close-ended questions, using the likent scale of 1.0 strongly agree, 2.0 agree, 3.0 neutrial, 4.0 disagree, 5.0 strongly disagree. Face validity of the questionnaire was performed to ensure the relevance of content and interpretation by discussing with experienced faculty members of experts in the field.

Table 2: Data Coding

Customer response	**Code of organization and presentation**	**Code Analysis**
Strong agree	SA	1
Agree	A	2
Neutral	NT	3
Disagree	DA	4
Strong disagree	SD	5

DISCUSSION AND FINDINGS

table 1 .**Marital Status**

	Frequency	Percent	Valid Percent	Cumulative Percent
married	27	56.3	56.3	56.3
divorced	7	14.6	14.6	70.8
single	13	27.1	27.1	97.9
others	1	2.1	2.1	100.0
Total	48	100.0	100.0	

From table it indicates that 53.3% are married,14.6% divorced, 27.1% single and 2.1 own the small and medium enterprise for the selected sample size. Hence more half of the sample are married and they own the business as family project.

How long have you been in business?

	Frequency	Percent	Valid Percent	Cumulative Percent
less than 5 years	26	54.2	54.2	54.2
5-8 years	11	22.9	22.9	77.1
8 years and above	11	22.9	22.9	100.0
Total	48	100.0	100.0	

From table 3 above majority of the respondents have been operating business enterprises for a period of less than years that is 54.2% have been in the business for less than 5 years, 22.9% have been in business for 5-8 years while above 8 years comprises of 22.9%.

What type of ICT device do you often use in your business

	Frequency	Percent	Valid Percent	Cumulative Percent
computers	25	52.1	52.1	52.1
phones, tables	22	45.8	45.8	97.9
Others	1	2.1	2.1	100.0
Total	48	100.0	100.0	

Form the data collected it indicated that most sme’s use computers and phone/tablets to manage their records, communicate and for inventory purpose. That 97.9% while 2.1% use other devices.

Security issues experienced by sme's

Loss of data while on transit

	Frequency	Percent	Valid Percent	Cumulative Percent
strongly agree	14	29.2	29.2	29.2
Agree	15	31.3	31.3	60.4
Neutral	10	20.8	20.8	81.3
disagree	7	14.6	14.6	95.8
strongly disagree	2	4.2	4.2	100.0
Total	48	100.0	100.0	

From the table, it shows that 29.2% strongly agree that there is loss of data while on transit, 31.3% agree, that amount to 60.4% who strongly and agree. While 20.8% are neutral,14.6 disagree, strongly disagree 4.2%

According to (Tuncay, 2019) Cryptography is important tool safe guard information that is transmitted using computers, phones and other computing gargets. Cryptography is the principles of encrypt and decrypt information into non-readable format so that only the authorized receiver can understand and use it. Cryptography is the art and science of coding crucial and confidential information from being accessed or used by non-authorized individuals. The main aim of cryptography is to protect and secure information from hackers, threats and cyber-attacks or users else other than the authorized receiver. Cryptography facilitates organizations to transmit data through the network, transferring important and private information securely. Hence cryptography allows users to adopt public or private media for example network to do business online while being protected and avoid being victims of criminals and password sniffers.

There are issues of data Loss encountered by the sme's

	Frequency	Percent	Valid Percent	Cumulative Percent
strongly agree	16	33.3	33.3	33.3
Agree	18	37.5	37.5	70.8
Neutral	4	8.3	8.3	79.2
disagree	9	18.8	18.8	97.9
strongly disagree	1	2.1	2.1	100.0
Total	48	100.0	100.0	

From the table above indicates that there are issues of data loss in the sme's which are attributed to a number of issues like, poor security mechanisms employed by the sme's, employee sabotage, various attacks to the storage devices.

Increasing complexity of infrastructure resulting in more time/effort for implementation and maintenance

	Frequency	Percent	Valid Percent	Cumulative Percent
strongly agree	13	27.1	27.1	27.1
Agree	22	45.8	45.8	72.9
Neutral	6	12.5	12.5	85.4
disagree	6	12.5	12.5	97.9
strongly disagree	1	2.1	2.1	100.0
Total	48	100.0	100.0	

It is noted that most respondents feel that there is increased complexity of infrastructure resulting in more time and effort for implementation and maintenance of the computing devices, 27.1% of the respondents strongly agree, 45.8% agree, 12.5% neutral, 12.5% disagree and 1% strongly disagree.

Inability to monitor data while in transit

	Frequency	Percent	Valid Percent	Cumulative Percent
strongly agree	16	33.3	33.3	33.3
agree	20	41.7	41.7	75.0
neutral	7	14.6	14.6	89.6
disagree	3	6.3	6.3	95.8
strongly disagree	2	4.2	4.2	100.0
Total	48	100.0	100.0	

From the table above it indicates that 33.3% of the respondents strongly agree, 41.7% agree, 14.6% were neutral, 6.3%disagree and 4.2% strongly disagree that they have inability to monitor data while in transit. Most respondents strongly agree and agree which comprises of 75% of the respondent.

Lack of staff with the skills to manage information security

	Frequency	Percent	Valid Percent	Cumulative Percent
strongly agree	14	29.2	29.2	29.2
agree	18	37.5	37.5	66.7
neutral	5	10.4	10.4	77.1
disagree	8	16.7	16.7	93.8
strongly disagree	3	6.3	6.3	100.0
Total	48	100.0	100.0	

From the table above it indicates that 29.2% of the respondents strongly agree, 37.5% agree, 10.4% were neutral, 16.7%disagree and 6.3% strongly disagree that they lack of staff with the skills to manage information security. Most respondents strongly agree and agree which comprises of 66.7% of the respondent.

My personal computer being hijacked over by a hacker

	Frequency	Percent	Valid Percent	Cumulative Percent
strongly agree	9	18.8	18.8	18.8
agree	17	35.4	35.4	54.2
neutral	10	20.8	20.8	75.0
disagree	11	22.9	22.9	97.9
strongly disagree	1	2.1	2.1	100.0
Total	48	100.0	100.0	

From the table above it indicates that 18.8% of the respondents strongly agree, 35.4% agree, 20.8% were neutral, 22.9%disagree and 2.1% strongly disagree that they lack of staff with the skills to manage information security. Most respondents strongly agree and agree which comprises of 54.2% of the respondent

Descriptive Statistics

	N	Mean	Std. Deviation
My data being corrupted by a virus	48	2.2292	1.17128
Risk of unauthorized access by insiders and outsiders	48	2.3958	1.06670
Risk of deliberate act of information access and use	48	2.3542	1.02084
Risk of an act of human error or failure	48	2.1667	1.05857
Risk of technical software and hardware failure or errors	48	2.2708	1.10588
Measures used by sme's			
Keeping spyware constantly updated and running on our devices	48	2.1250	1.12278
Keeping antivirus constantly running is important	48	1.8750	1.14157
Having antivirus protection	48	1.9792	1.08156
Using strong passwords on different devices	48	2.0000	1.18501
Using encryption techniques for files with highly confidential data	48	2.1250	.93683
Stop downloading from the unknown sources	48	2.0208	1.22890
Abiding with the information security policies	48	2.0833	1.02798
Have you taken your employees on information security awareness training?	48	3.1250	1.37802
Availability of the cloud computing services for data storage	48	2.9792	1.37593
Data Integrity of business data and information stored in databases	48	2.9375	1.32739
Confidentiality and privacy of data stored in data bases	48	2.8958	1.25883

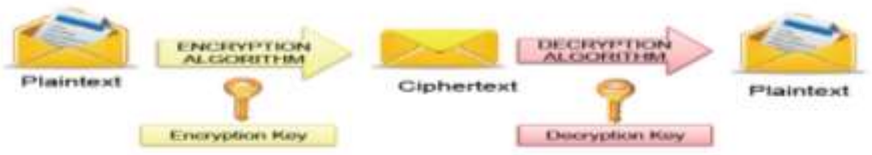
Form the table above it indicates that my data being corrupted by a virus with a mean of 2.2292 and standard deviation of 1.17128 that implies that most respondents strongly agree that data is being corrupted with virus. According to (Dashora, 2011),Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it.

Risk of unauthorized access by insiders and outsiders with a mean of 2.3958 and a standard deviation of 1.066670 implies that most respondents strongly agree that data is being corrupted with virus. Risk of deliberate act of information access and use with a mean of 2.3542 and a standard deviation of 1.02084 implies that most respondents strongly agree that risk of deliberate act of information access and use. Risk of an act of human error or failure with a mean 2.1667 of and a standard deviation of 1.05857 implies that most respondents strongly agree that risk of an act of human error or failure. Risk of technical software and hardware failure or errors with a mean of 2.2708 and a standard deviation of 1.10588 implies that most respondents strongly agree that Risk of technical software and hardware failure or errors.

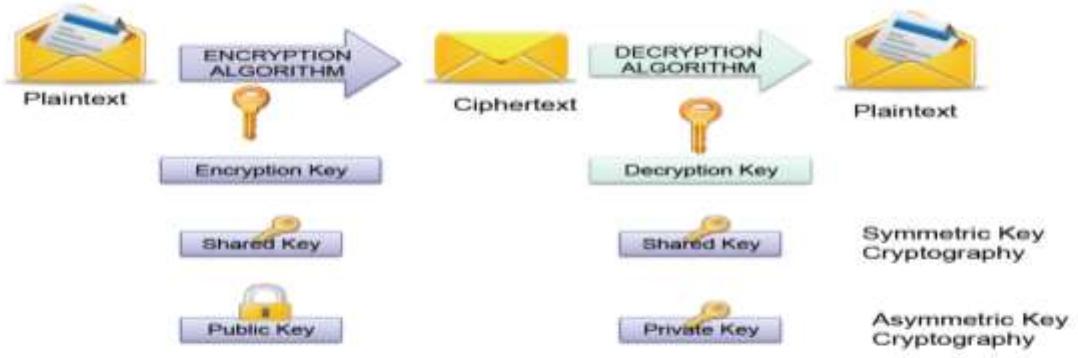
Measures used by sme's in east Africa

Using encryption techniques for files with highly confidential data with the least mean and standard deviation, mean of 2.1250 and a standard deviation of .93683 implies that most respondents strongly agree that Using encryption techniques for files with highly confidential data.

Encryption and decryption



Symmetric and asymmetric keys crptography



There is a history of cryptography being used before the Christian era. The Roman ruler Julius Caesar (*100*BC-*44*BC) adopted a cipher for secret communication between his army. This is a class of substitution cipher wherein a rule is to substitute each letter by another letter of the alphabet. It included the substitution each letter of the alphabet with a letter five points further down the alphabet. Later any cipher that used this substitution concept for creation of a cipher alphabet was referred as a Caesar cipher. Of all the substitution type ciphers, the Caesar cipher was the simplest to solve as it has only 25 possible combinations. The encryption can also be expressed by modular arithmetic. The letters of the alphabets are first represented by numbers with $A=1, B=2\ldots Z=26$. The encryption of a letter x can be with shift n can be expressed mathematically as, $En(C) = (P + K) \bmod 26$ Decryption is performed similarly by, *Dn (C) = (P-K) mod 26* (Shukla, 2016). For example if the plain text is"MAN" and key =5

Solution: ENCRYTION

C(M)=(13+5)MOD 26

18 MOD 26

C(A)= R

C(M)=(1+5)MOD 26

6 MOD 26

C(A)= F

C(M)=(14+5)MOD 26

19 MOD 26

C(N)= S

PLAINTEXT= MAN

CIPHER TEXT= RFS

CONCLUSIONS AND RECOMMENDATIONS

The adoption and use of ICT in small and medium enterprises it increased the growth of information security issues, security needs to be analyzed regularly. The end Users should be aware of the risks and vulnerabilities present in the current information technology age and in there computing platforms before being a part of that platform. Confidentiality and privacy concerns were identified as an associated concern with security issues in sme's. Encryption is suggested as a better solution to secure information. Before storing data in cloud server and other storage devices, it is better to encrypt data. Data Owner can give permission to particular group member such that data can be easily accessed by them. To avoid access of data from other users, applying encryption on data that makes data totally unusable and normal encryption can complicate availability.

REFERENCES

1. Abbas, J., Mahmood, H. K., & Hussain, F. (2015). INFORMATION SECURITY MANAGEMENT FOR SMALL AND MEDIUM SIZE ENTERPRISES. *Sci.Int.(Lahore)*, 2393-2398.

2. Aleksandar, E. (2019). INFORMATION SECURITY: THREAT FROM EMPLOYEES. *TECHNICAL JOURNAL*, 123-128.

3. Alhassana, M. M., & Adjei-Quaye, A. (2017). Information Security in an Organization. *International Journal of Computer* , 100-116.

4. Amarachi, A., Okolie, S., & Ajaegbu. (2013). Information Security Management System: Emerging Issues and Prospect. *IOSR Journal of Computer Engineering*, 96-102.

5. Chen, T. M. (2009). Information Security and Risk Management. In M. Pagani, *Encyclopedia of Multimedia Technology and Networking*. Idea Group Publishing.

6. Dashora, K. (2011). Cyber Crime in the Society: Problems and Preventions. *Journal of Alternative Perspectives in the Social Sciences*, 240-259.

7. Erceg, A. (2019). INFORMATION SECURITY: THREAT FROM EMPLOYEES. *TEHNIČKI GLASNIK*, 123-128.

8. Gençoğlu, M. T. (2019). Importance of Cryptography in Information Security. *IOSR Journal of Computer Engineering*, 65-68.

9. Laybats, C., & Tredinnick, L. (2016). Information security. *Business Information Review*, 76-80.

10. Negash, S. (2019). Factors Hindering Full-Fledged Information Security in Banking Sector in Ethiopia: Emphasis on Information Security Culture. *Twenty-fifth Americas Conference on Information Systems*, (pp. 1-10). Cancun.

11. Shukla, K. N. (2016). Aryabhata and the Information Security. *International Journal of Innovation in Science and Mathematics*, 81-84.

12. Singh, A. K. (2017). Security and Management in Network: Security of Network Management versus Management of Network Security (SNM Vs MNS). *International Journal of Computer Science and Network Security*, 166-173.

13. Surwade, Y. P., & Patil, H. J. (2019). INFORMATION SECURITY. *An International Peer Reviewed Bilingual E-Journal of Library and Information Science*, 458-466.

14. Tuncay, G. M. (2019). Importance of Cryptography in Information Security. *Journal of Computer Engineering*, 65-68.

15. Woretaw, A., Lessa, L., & Negash, S. (2019). Factors Hindering Full-Fledged Information Security in Banking Sector in Ethiopia: Emphasis on Information Security Culture. *Twenty-fifth Americas Conference on Information Systems*, (pp. 1-11). Cancun.

16. Zhi, X. (., & Atif Ahmad, S. B. (2013). INFORMATION SECURITY MANAGEMENT: FACTORS THAT INFLUENCE SECURITY INVESTMENTS IN SMES. *austarian information security management conference*, 60-74.