American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-9, Issue-3, pp-258-267
www.ajer.org
Research Paper Open Access

Evaluation of Failure and Success Factors for Information System Security Management

Aru Okereke Eze, NNAMDI HENRY I.

Department Of Computer Engineering, Michael Okpara University Of Agriculture, Umudike Umuahia, Abia State-Nigeria.

Department Of Computer Engineering, Michael Okpara University Of Agriculture, Umudike Umuahia, Abia State-Nigeria.

ABSTRACT: *An Information System Security Management (ISSM) is the critical issue and aspect of an information system as the venerability rate of data and information increases. An evaluation of the failure and success factors for information system security management will help in identifying crucial factors that need critical attention and consideration in other to build a strong an impenetrable information system that will guarantee the core principles of data communication including confidentiality, integrity and authenticity of data managed in such system. The objective of this paper is to explore the reasons for failures in the information system and x-ray the success strategies employed in the systems that has so far proven to be efficient in terms of information system security management. The evaluation of the success and failure factors was carried out with data collected by means of questionnaires. From the results and findings, amongst the success factor categories considered,Security management practices, Culture, Environmental influence and Organizational structure, the one with the highest response is the security management practices as detailed in the work. Also failure factors categorized into Project failure, System failure and User failure were considered and the user related failure factors was evaluated to be the factors that has the highest rate of influence on ISSM. Conclusively, evaluating the success and failure factors in ISSM is essential as it provides a useful indicator of essential security management practices required in a businesses, organisations and offices.*

KEYWORDS: *Evaluation, Information, System, Security, Management, etc*

Date of Submission: 01-03-2020 Date of acceptance: 21-03-2020

I. INTRODUCTION

Information is an asset, and having specific, relevant and correct information can make a massive difference to an organization's efficiency (Maryam Al-Awadi, Karen Renaud 2014. For many organisations, information is their most important asset, so protecting it is crucial.

Information security is “the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information”. Information can take many forms, such as electronic and physical(Nicholas King 2019). Information security means protection of information against various threats in such a way as to ensure business continuity, minimize losses, and maximize return on investments and business activities. (Tomasz Chajduga 2019). However, information security does not cover only the information itself but also the entire infrastructure that facilitates its use and the factors. It covers hardware, software, threats, physical security and human factors, where each of these components has it is own characteristics. Consequently information security plays a major role in the internet age of technology.) Information security, sometimes usually shortened to InfoSec, is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of informationgiven that the number of organization security breaches is increasing daily, and the more accessible the information, the greater the hazards, it is inevitable that security will need to be tightened (Brown & Duguid, 2000). As the number of employees, applications and systems increase, the management of the organization’s information becomes much more difficult and consequently vulnerabilities potentially increase, hence the need for a better security management system.

This paper is organised as follows. The next section presents an overview of ISSM, followed by the review of past literatures. The methodology used to collect and analyse the theoretical and empirical data was discussed, then the nest section presents the findings of the analysis and discussion on the implications. Finally, the summary and concludes.

Information Systems Security Management (ISSM).

Information Systems Security Management (ISSM) from the emergent organization perspective e.g. the e-commerce is a way under study and requires attention from the academician (Azah Anir Norman and Norizan Mohd Yasin,2010). Information system can be compared to the nervous system. To malfunction in one place can cause failure of the entire organization and its exposure to risk of loss or a fall. Therefore, maintaining high performance information system, including the appropriate level of security, may have a direct impact on how organizations respond to crises. (ISSM refer to the whole process of managing IS security encompassing three characteristics. These characteristics are people, technology and procedures. ISSM is important because it is cost-effective to view business's IS security plan and management from IS security point because issues such as people and procedures are addressed as important as the technical measure in securing company assets. It is utmost important to critically review the ISSM implementation in hierarchical organization and the emergent organization to provide a background understanding of the current situation of ISSM practice today. It is also the grounding work for the research to identify gaps in the current academic research thus proposing a suitable solution to close these gaps. Stable organizations or also known as hierarchical organizations usually demonstrate characteristics such as having tier or level in its management structure, where clear governance of accountability and procedure at every tier or level is observed. They also have long life span in terms of system and applications for the purpose of information dissemination and usage. They are usually rigid in structure and processes with very strong showcase of organizational stability in terms of management and resources. As for emergent organization, the situation is opposite. Emergent organizations showcase every feature of social organizations culture, meaning, social relationships, decision processes and so on, are continually emergent, following no predefined pattern what so ever. Emergent organizations also display constant social negotiation and consensus building in its business structure and processes. It may exhibit temporal regularities but none is long life as compared to the hierarchical organization. Although some emergent organizations may be smaller in size and resources, the threats on the information systems is very much similar and disastrous as compared to the stable organizations. Protecting information or better say reassuring security is not just a technology issue anymore. Lately, vast importance is given to actions, plans, policies, awareness that companies, organizations or individuals take to protect information. It is said that “Information security is not an 'IT problem' anymore, it is a business issue.

II. REVIEW OF RELATED ARTICLES ON INFORMATION SYSTEM SECURITY MANAGEMENT

Management information system can be compared to the nervous system of a company. Its malfunction may cause adverse effects in many different areas of the company. Information Security Management is understood as tool of the information confidentiality, availability and integrity assurance. An effective information security management system reduces the risk of crisis in the company. It also allows to reduce the effects of the crisis occurring outside the company Slawomir Wawak (2010) Information Systems Security Management (ISSM) today plays an important role in any organization security implementation (Posthumus and von Solms, 2004).Information Systems Security is defined as the broader view of computer security term, incorporating system analysis and design methods, manual information systems, managerial issues and both societal and ethical problems, the same article asserts, computer security connotes threats concepts and the physical and logical techniques applied in protecting the electronic computer and communication systems. Definition above clearly shows IS security encompasses a broader perspective as compared to computer security (technical oriented). Thus, in this challenging business world today, it is far more cost-effective to view business's IS security plan and management as issues such as people and procedure are addressed as important as other technical measure in securing company's asset. Although this concept has been made clear above, in actual practice however, the adoption and implementation of ISSM is still very low.

In the recent Deloitte's annual telecommunications (TMT) security survey it was found that 32 per cent of respondents have reduced their information security budgets in the past year. There are many plausible explanations to this situation and one glaring reason is low management concern about IS security. To raise management involvement in IS security decisions, it is important to convince managers about the benefits of IS security efforts and let them know types of IS security measures that are effective depending on organizational circumstances. Using traditional approaches as IS security effort are no longer suitable as most of the traditional approaches focuses on technical fixes, which are not pliable with the dynamic nature of business today. The management has to picture IS security effort in holistic point of view and not consider IS security as just another commodity, but sees IS security effort as a booster to the business and the business image among business competitors. Information security is not a new field. Information security has a very long history even4before the computer existed. Information security,for instance encryption, has been used since humanknows how to write. Information security todayencompasses more complex scenario compare to theolder days. The introduction of computers togetherwith the development of the Internet technology haschanged how we handle and secure information.

Today many information systems are created to handle sensitive information for the benefit of organizations. The evolving technology and new business arrangement in distributing information has made it vital for all business owners and business management to consider IS security effort. One effort that has been discussed in great extends by IS researchers are in the field of ISSM commonly based on standardization namely the BS ISO/IEC17799:2000 (Azah Anir Norman and Norizan Mohd Yasin,2010). This standard is widely adopted by large organization for their competitive advantages. The adaptation of ISSM not only serves to manage organizations' IS Security resources, but this exercise certifies the organization as being capable of managing its IS Security in the enterprise-wide environment. By being certified, organization is verified (by the standardization body) competent in managing IS security, thus creating a better position for the business in the market among its users. This effort may sound easy as detailed guide is provided from the standard, but in actual fact, it takes years to exercise all the processes in the standards, thus making it part of organizations' business process and policy. (Azah Anir Norman and Norizan Mohd Yasin,2010)

Although there are many major standards such as BS ISO/IEC17799: 2000, Generally Accepted Information Security Principles (GAISP), Systems Security Engineering Capability Maturity Model (SSE-CMM) and Standard of Good Practice for Information Security available, most of them fail to look into the content of the standard. All of the standards focus on the existence of process where no further advices were given to assist the practitioner. Because of this scarcity, the applicability of this standardization toward business becomes tough and timely. The inflexibility of the chosen standards to a business is also questioned. The same scarcity also elevated issues on how well the security activities are carried out in an organization, and how exactly the objectives are to be achieved in organizations. For these reasons, it may provide a false sense of security in an organization. Besides these scarcities, most of the standards are built based on hierarchical organizational experience, practice and structure, which are inflexible and has rigid structure. As the business orientation and business objectives between the hierarchical organizations and the emergent organizations are different, using the current standards to achieve ISSM in e- Commerce Company will be difficult.

2.1Theoretical Perspectives of Information Systems Security Management (ISSM) Success Considerations

Determining success factors in ISSM is essential as it provides a useful indicator of essential security management practices required in a business. This indication will provide a general idea to the e-commerce companies to adopt appropriate ISSM for their businesses. Consequently from this determination, e-commerce Company could invest on proper ISSM practice which is achievable with the business objectives. Thus, only required resources are used and utilized without waste. Besides giving information to the organization on how to stay safe and secure in the business, ISSM success factor also demonstrates the successful elements business must anticipate to preventing IS failure. Today, almost all businesses rely particularly in IS. Bound to IS is the essential information of the business, where security management is inseparable feature to ensure business stays safe and secure.

The organizational factors are again used in Kankanhalli et al. (2003) study of information system security effectiveness. She found that similar factors are applied in determining IS security effectiveness. Because this study looks at e-commerce as the organizational context in the study of information systems security management success factors, similar organizational factor is also considered and is accepted as part of attributes to be analysed. The choice of these two theories is mostly made due to the logical connections it has towards being successful. In many IS implementations, consideration on adopting the related innovation is seen as a positive influence determining successful IS management. In the context of this research, innovation is referred to as ISSM.

The reason is because ISSM is an innovative process, guaranteed to improve current business process, thus adds values. Theories referred to on the IS adoption are the Diffusion of Innovation (DOI) by Rogers (1983) and Technology-Organization-Environment Framework (TOE) by Tornatzky and Fleisher (1990). Rogers (1983), Cooper and Zmud (1990) and Agarwal and Prasad (1998) each agreed that the relative advantage, compatibility and complexity of innovation are the antecedents towards an innovation adoption. These three antecedents make up DOI as a theory. These three antecedents determine the intention of adoption by a business, thus establishing a successful implementation. Through an effective implementation, a successful security management could be achieved. TOE expressed that in order to decide on an adoption, factors influencing adoption are somewhat relevant. In Tornatzky and Fleisher (1990) and Tornatzky and Klein (1982), technology, organization and environment (TOE) are distinguished as opportunities and constraints towards innovation adoption. These three are influencing factors significant in any businesses and applicable to all businesses that leverages IS including the e-commerce business. Concisely, TOE makes up the whole concept to determine success factor in this research. Another significant IS success theory considered to be motivating the entire research scenario is the IS Success Model (DeLone and McLean, 1992) which looks at attributes evaluating successful IS implementation and practices. This theory highlight six IS success categories which are system quality, information quality, user, user satisfaction, individual impact and organizational impact. In conclusion, IS success attributes are grouped appropriately under the Technology-Organization-Environment Framework, hence, depicts the theoretical model of this study.

Information systems security management (ISSM) connotes the holistic security management in a business. ISSM looks at people, process and technology issues of a business environment. It is necessary for a business to look into people, process and technology perspectives (James, 1996). This is because information systems are not just about the technology, but the people- creator and users, and process-involving internal and external environments of related business. It is most appropriate and logical to use the theoretical model developed, because it supports the bigger picture of ISSM concept. The challenging part is to accommodate the attributes in each theory to suit the TOE umbrella, which is discussed separately in this article. The ISSM is very much associated with the e-Commerce, not just because it involves information systems, but its life-existence is supported by the Internet. As the Internet is exempted from controls, appropriate ISSM is highly needed to ensure safe and secure transactions between users and the business entity, thus providing trustworthy information systems. Security management signifies the process of implementing and exercising security measures appropriate towards a business with the objective to mitigate risk and threats. Security management must also decide on business in attempts to withdraw any security measures due to change of business objectives or upgrade of the information systems. The same security management exercise and meaning is reflected in many security standards and best practices including ISO27002, GIASP and Standard of Good Practices. Many scholars also discuss similar meaning of security management in their papers (Dhillon and Backhouse, 2000; Dhillon, 1995; Eloff and von Solms, 2000; Finne, 1998; Hong et al., 2003; Jan and Mariki, 2003; Kritzinger and Smith, 2008; Sanchez et al., 2006; Siponen and Willison, 2008; von Solms, 2006; von Solms and von Solms, 2004; Zuccato, 2007) Thus, it is justly to say that security management involves businesses to implement, exercise and monitor appropriate security measure to protect and safeguard business assets in the business information systems. Security management also justifies the means of implementing security measure appropriate to business objectives, thus eliminates abuse and wastage of business resources.

Reflecting on the security management meaning, there are so much to be done to qualify company to be a wise security management user. There is no rule of thumb but there are many considerations to it such as highlighted by von Solms and von Solms (2004). Besides security management consideration, business is also bound to the return of investment (ROI) objective for its survival. Hence, business must make smart decisions in implementing appropriate security management measures. It is also vital that the security measures imposed be in line with the business objectives therefore, show security management effectiveness. Besides, it is also crucial for a business to know and understand business IS usage to execute everyday work, so that appropriate security measures are implemented. In an increasingly interconnected environment, information is exposed to a growing number and wider variety of risks. Threats such as malicious code, computer hacking and denial-of-service attacks have become more common, ambitious and sophisticated, making implementing, maintaining and updating information security in an organisation more of a challenge.(Nicholas king 2019).There are many frameworks of security management practices (Eloff and von Solms, 2000; Finne, 1998; Lech, 2000; Trcek, 2003; von Solms, 2005; Zuccato, 2007), to help them in their security management implementation. There are piles of references such as the security standards and best practices for business to learn from, but standards and best practices could take some time to read and comprehend. This is because standard does not specifically provide step-by-step content towards implementing security management (Siponen, 2006; Zuccato, 2007). Standards too are mostly developed based on conventional business or hierarchical business where approach may not be suitable for the e-commerce business today (Baskerville and Siponen, 2002; Zuccato, 2007).

III. RESEARCH METHODOLOGY

In this study, we used simple descriptive survey approach, data collection and analysis was done using the Questionnaire and is represented in charts and graphs using the excel. Descriptive research, or survey research, determines and describes the way things are. It involves collecting data to test hypotheses or to answer questions about people's opinions on some topic or issue.The six major steps in carrying out a descriptive research as used in this work are;

- Identify problem
- Review literature
- Select participants and instruments
- Collect valid and reliable data
- Analyse data

- Report conclusion

Papers are selected from conference proceedings and distinguish journals which varies from the conceptual to the empirical research .The scope of the Selected papers are according to the ISSM discussion in large and small business context. The selections of papers look at the extensiveness of ISSM discussion covered in the articles. Issues and findings related to ISSM are critically analysed using empirical data or conceptually discussed. Several articles were selected for this evaluation and discussion. The chosen articles were systematically reviewed based on the characteristic factors discussed in this journal .The analysis evaluates and identified the mentioned characteristics of the security management model reflecting what is documented with what is being practiced. This step is conducted to distinguish the most frequent characteristics deemed to be necessary for ISSM. A reflection of the whole findings (depicted in the Table matrix) with the ISSM success considerations theoretical model is then carried out for final analysis in this study. The reflection should establish the basis of successful ISSM, which is supported by the ISSM theoretical framework outlined earlier. Based on the summary of the ISSM model, tables and charts are drawn up to represent the findings and analysis of the review

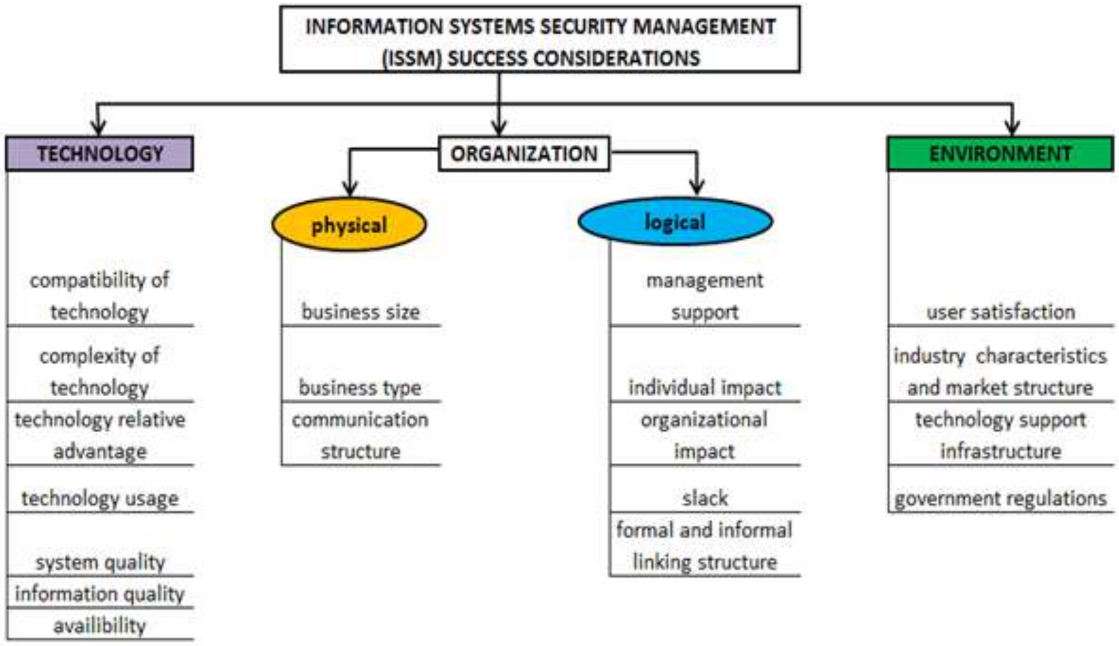

Figure1depicts the ISSM Success Considerations (Azah Anir Norman and Norizan Mohd Yasin ,2013)

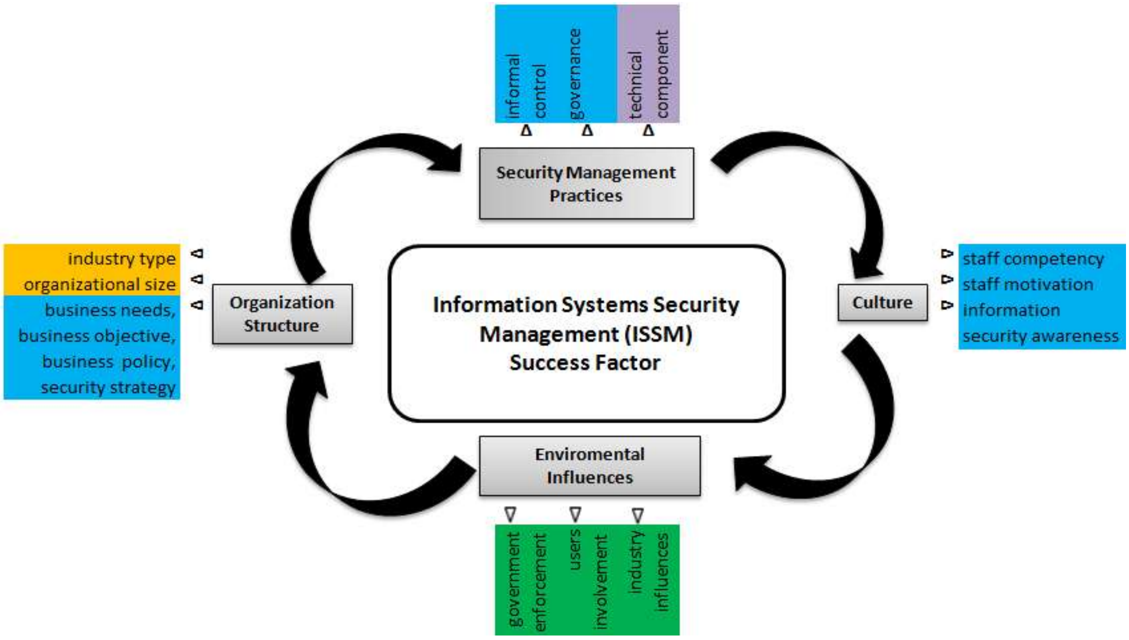

Figure2: ISSM Success factors(Azah Anir Norman and Norizan Mohd Yasin ,2013)

The main entities that umbrella the whole security factors are technology, organization and environment factors. Under the organization, two characteristics were defined which are the physical stance and logical stance. Under each entity lies the attributes deem to be crucial towards determining success factor of ISSM for this study. Technology is emphasized on the systems itself, thus from here on called systems characteristics. Under physical organization, it looks at organization’s physical existence such as, size type and the communication structure. As for logical organization context, it emphasized on the logical factors such as management support, individual and organization impact. Under the environment, it considers the user satisfaction, industry characteristic, market structure, and technology support and government regulations. Organization gives emphasize on the context/business entity while the environment looks at the surrounding of systems and the context/business entity.**Figure** 1 act as a reference in building an ISSM success factor model.

Evaluation of the Success Factors of an ISSM

In the evaluation of the Success factors as shown in Table 2 and represented in Figure 3 as pie chart that shows pictorially the percentage of the response gotten from a questionnaire.The questionnaire was used to evaluate the rate at which the under listed success factors affect a chosen information system security management organization .Generally the success factors was classified into four categories,(Azah Anir Norman and Norizan Mohd Yasin,2013) namely;

- Security management practices, with factors such as Informal control, Governance and Technical component
- Culture, with factors such as staff competency, staff motivation and Information security awareness
- Environmental influence, with factors such as Government enforcement, User involvement and Industry influences.
- Organizational structure,with factors such as Industry type, Organizational size and business need.

In determining the rate at which the above listed factors affect the operation of an Information system security management organization, one hundred questionnaires was shared to information security management experts from a selected IT organizations to obtain responses from them as regards to the rate at which the above listed success factor affect the ISSM of their organization. This was the question in the questionnaire.

Which of the following success factors do you consider as having the highest effect on your ISSM?

1) Security management practices
2) Culture
3) Environmental influence
4) Organizational structure
5) Budget

Table 1 below shows the responds received from the above question.

Table 1: Percentage consideration of success factors on ISSM

Factors	**Response**	**Percentages**
Security Management Practices	35	35%
Environmental influence	27	27%
Organizational structure	15	15%
Culture	23	23%
TOTAL	**100**	**100%**

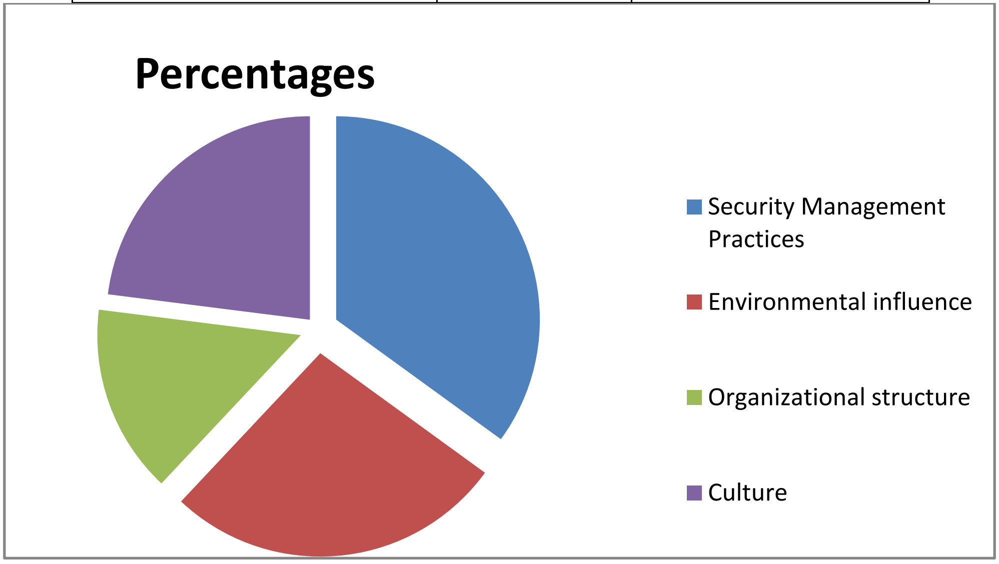

Figure 3: (A pie chart showing in percentage, the responses made on the different factors as contained in the questionnaire)

2.2 The Critical Failure Factors of an Information System Security Management

Failure rate of ISSM have rapidly increased in different aspects due to different reasons, ranging from administrative policies to carelessness in the management of critical data and then increasing number of threats to information security posing great challenge to the management of information by various organizations which can be described as a failure factor as it hinders the effectiveness and efficiency of an information system security management. Although above situation is not a new sight in the field of Information System, it creates many obstacles to regular activities of any organization. The failure of Information System has become a common state for any organization or industry and not depending on their rank or status. Numerous factors may have affected ISSM failures and these factors are functioning together or individually to create the failure situation of Information Systems.The main failure factors that ISSM based on literature are; environment, quality control, human related, technology related and other connected factors. It can be mainly divided into two parts. They are conceptual factors and background factors or hard factors and soft factors. User participation, participant behaviour, user satisfaction, attitudes and expectation level, and the management of organization, infrastructure facilities and pattern of usage play a crucial role in the field of Information Systems that have been identified as background factors with significant impact on Information System failures. Quality failure, project failure, system failure, management failure and software failure are identified as conceptual failure factors.

Evaluation of Failure Factors of an ISSM

The failure or success of an ISSM is determined from the people since they use the system .When a system developed with certain expectation fails to meet up with the performance requirement, and then the system has failed .The various constraints or factors can be used to evaluate the rate of success or failure of an Information System Security Management.

Evaluation of the Failure factors as shown in Table 2 and represented in Figure 4.a (a bar chart that shows pictorially the percentage of the response gotten from a questionnaire). The questionnaire was used to evaluate the rate at which the under listed failure factors affects a chosen ISSM organization .In the evaluation the failure factors, were generally classified into three categories;Project failure, System failureand User, failure In determining the rate at which the above listed failure factors affect the operation of an ISSM, one hundred (100) questionnaires was shared to information security management experts from selected IT organizations to obtain responses from them as regards to the rate at which the above listed failure factor affects the ISSM of their organization. This was the question in the questionnaire.

➢ **What is the best classification of your observed failure factors in the ISSM of your organization**
- Project failure
- System failure
- User failure
- Insufficient Budget

Table2: Tabulation of Failure Factors with their percentage response

Factors	Response	Percentages
Project failure,	18	18%
System failure	19	19%
User failure	24	24%
Insufficient Budget	39	39%
Total	**100**	**100%**

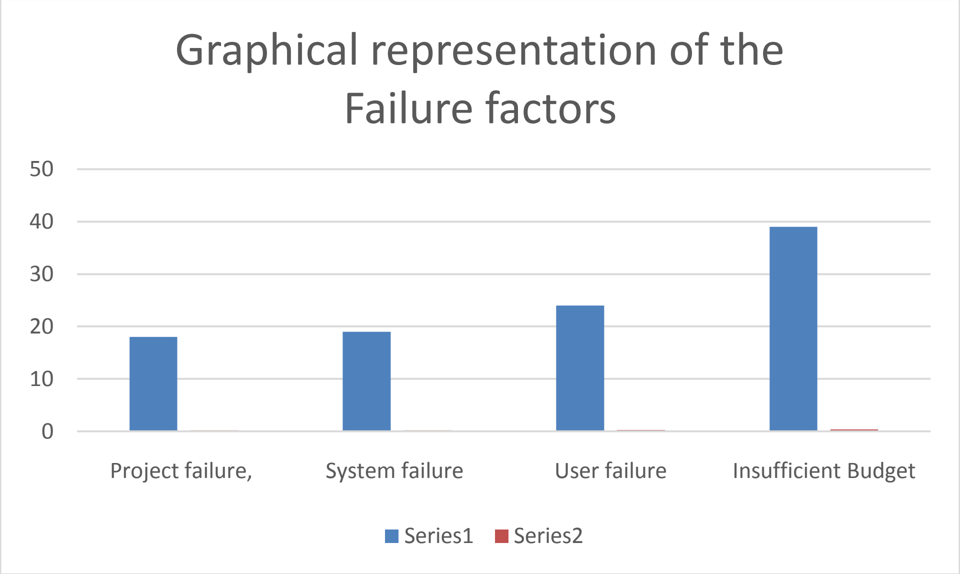

Figure 4 (A bar Chart representing the responses in percentage of the four categories of failure factors)

These factors as well as factors that have minor importance should be considered seriously. The main task of information security management is to give us confidence that, the security requirements that have been imposed on the system are adequate to protect data and resources (Mehdi Kazemi et al, 2012). Another task is to ensure that ISSM is working somehow to meet the security needs and reports important deviations in security (Marshall et al., 1995).

Critical failure factors of an ISSM are described by Ganesh & Mehta 2010) as follows.

1. Lack of consultant effectiveness
2. Low quality BPR (Business Process Reengineering)
3. Ineffective project management
4. Misfit of IS Software
5. High turnover rate of project team members
6. Over-dependence on intense customization
7. Insufficient IT Infrastructure
8. Lack of knowledge in transfers
9. Ambiguous Concept of the Nature of IS
10. Unclear concepts of IS from the Users perspective
11. Impractical expectations from top management from IS projects
12. Too firm project schedule
13. Users’ resistance to change
14. Lack of top management supports
15. Low quality of testing
16. Informal strategy

17. Unprofessional dedication
19. Functionality problems with the system
20. Overrun costs

IV. DISCUSSION

ISSM Success and Failure Factors

Evaluating the critical success and failure factors of an ISSM is step towards the right direction.This study proposes a theoretical model to investigate main factors that contribute to successful information security management and mitigate as far as possible the failure factors enumerated. By reviewing the ISM standards and literature in IS field, many critical success factors are identified and the relationship among these factors are proposed.

From The results obtained from the responses through the questionnaire as tabulated in the table above reveals that with Security management practices, culture, environmental influences, organizational structure as detailed above information security controls can be effectively developed, resulting in success of information security management.

What has been discovered from the study is that there are a number of essential factors which information security experts have identifies as being essential if an organization wants to achieve a level of information security. Implementation of information security won't be possible if a sufficient budget is not allocated. Furthermore, we hope that clear organizational mission statements and goals result in positive employee behaviour and positive attitudes towards securing the organization's information assets. The results suggest that the identified factors are connected and linked to each other and therefore it is difficult to prioritize one factor over another.

It is very likely that the factors identified by this study would have a significant impact in helping organizations to achieve effective information system security management. When adhered to, these factors should lead to fewer security breaches within the organization. While the study highlighted the requirements for good information security practice there is a need for follow-up studies using different methods or different tools to help organizations to understand what is required to improve the effectiveness of their information security policy.

This study is expected to contribute to both academics and management practice. Theoretically, this study proposes a theoretical model of successful information security management that can be empirically tested. While practitioners have developed information security standards and guidelines, both theory clarification and rigorous empirical studies are strongly needed in the academic area. Practically, the points and results of this research will help organizations better implement ISSM. With the identification of critical success and failure factors, managers can focus on the key issues to ISSM success and better arrange limited resources to secure the implementation of ISSM. Further, the potential empirical test of this study can provide manager with a way of evaluating the reliability or objectivity of the claimed best practices in practical standards and guidelines.

This study provides recommendations for future research avenues. First, empirical study needs to be conducted. The theoretical model is developed through literature review and has never been tested. The model's reliability and validity need support from empirical studies. Second, as little empirical study has been done on information security management from organizational level, the operationalization of all constructs needs to be developed and further validated. Finally, stronger theory base is needed to further Support this research model.

V. RESULTS &DISCUSSIONS ON THE SUCCESS FACTORS

Out of the 100 hundred questionnaire responses obtained, 35 responses which represent 35% of the entire responses were obtained for Security Management Practices. This signifies that majority of the respondents believe that the successes recorded in their ISSM has a lot to do with the security management practices they undertake. With this view when proper attention is placed on enhancing the security management practices, more success will be recorded in ISSM.

Also the Environmental influences got the second highest response with 27 responses which represents 27% of the total entry. This also signifies that individuals and organisation places considerations on factors that relates to the environments. For instance an organisation that is situated in an IT based environment will have access to better security management strategies that ones who are situated in a local environment. With these responses if more considerations are place on the Environment a factor in improving the ISSM success, then a significant increase will be recorded.

The other factors that also obtained responses from respondents are the Organisational structure and the culture. Organisation structure from the respondents view was seen to have 15 which represents 15% of the entire responses while the culture got 23 which represent 23% of the entire responses. The way an organisation is structured determines to an extent the success obtainable in their ISSM. Some organisations places security levels on the personnel depending on the rank and status of the person. Hence when an organisation has such structure, it to a great extent increases the ISSM of such organisation. Therefore, since with better organisational structure a company records more success in its ISSM, it is therefore recommended that organisations should practise a structure that allows for security level placement on staff and personnel according to their levels, ranks and responsibility.

As regards to culture which is the organisational way of life, i.e the practices that are obtainable in the organisation. Organisations that has better information security practises will experience more success in their ISSM and this can be inculcated through trainings and seminars on modern information security practices.

Results & Discussions on the Failure Factors

Insufficient Budget: From the responses as obtained from respondents, it is observed that insufficient budget had the highest percentage with 39 responses representing 39% of the entire submission, meaning that majority of failure of the information system security management are related to the insufficient supply of fund. With this finding, if organisations can consciously improve on the allocated budget for information security management, then there will be significant reduction in failures of the ISSM as relating to finance factor.

The Project and System failure follows in descending order of their percentage rate of effect on ISSM.

User failure: When the user is resistant in using the system, it is called user failure. The reason may be lack of training and ability of staff, complexity of the new system or a confrontation against a new system. From the responses, 24 respondents which represent 24% of the total response believe that the major cause of failure in ISSM is from the inability of users to effectively utilize information management systems and apply all the necessary security ethics required. In other to reduce to the minimum failures relating to users of an ISSM, Organisations should increase the staff training in order to make their personnel's have a mastery of the system.

Project failure: When the approved standards have not been met, it is called project failure; It includes not meeting the deadlines, budgets and the functionality. From the responses, 18 respondents which represent 18% of the total response believes that project failure contributes to the failure in an ISSM. Organisations in this regard will ensure that the set project deadline, budget and functionality are meet,this can be achieved by defining properly the scope of an ISSM project and ensuring that the estimated funds are duly released.

System failure: When the system does not perform as expected and also does not operate at the particular time or not being used in the way intended it is called system failure. The projects may not produce productive gains even when they are used with right intentions. From the responses as obtained from respondents, system related failure had 19 response which represents 19% of the entire entry. Managements in organisation can have this in mind while making decisions on purchases of equipment and devices used in ISSM, to ensure that system with high efficiency are used in ISSM. This will to a high extent reduce the failures associated to system malfunctions in an ISSM

REFERENCE

[1]. Azah Anir Norman and Norizan Mohd Yasin,(2013) " Information systems Securitymanagement (ISSM) success factor: Retrospection from the scholars" African Journal of Business Management.

[2]. Azah Anir Norman, Norizan Mohd Yasin, (2010) "A Critical Review of Information SystemsSecurity Management (ISSM) Implementation: Comparison between Stable Organizations and Emergent Organizations ,International Journal of Digital Society (IJDS), Volume 1**,**

[3]. Bikram Pal Kaur , Dr.Himanshu Aggrawal,(2013)"Critical Failure Factors in Information System :An exploratory review", Journal of Global Research in Computer Science,Volume **4,** No**. 1,**

[4]. Brown, J. S. and Duguid, P., (2002.) "The Social Life of Information". Boston, Harvard Business School Press**.**

[5]. D.N.T.Gunawardhana ,Chandana Perera (2015)"Classification of Failure Factors in Information Systems" International Journal for Innovation Education and Research Vol.3-3.

[6]. Gordon, L. A. & Loep, M. P. (2006). "Budgeting Process for Information Security Expenditures".Communications of the ACM, Vol. 49, No. 1.

[7]. Kankanhalli et al (2003) "An integrative study of information systemssecurity effectiveness" International Journal of Information Management 23 (2003).

[8]. Maryam Al-Awadi, Karen Renaud (2014) "success factor in information system security implementation in organizations" www.researchgate.net/profile/Karen_Renaud/publication/266231077

[9]. Mehdi Kazemi, Hamid Khajouei and Hashem Nasrabadi (2012) "Evaluationof information security management system success factors: Case study of Municipal organization" African Journal of Business Management Vol. 6(14).

[10]. Nicholas King (2019) "The importance of information security" https://www.vigilantsoftware.co.uk/blog.

[11]. Nurazean Maarop, Noorjan Mohd et el (2015) "Understanding Success Factors of an Information Security Management System Plan Phase Self-Implementation" World Academy of Science, Engineering and Technology International Journal of Computer and Information Engineering Vol:9, No:3, 2015

[12]. Slawomir Wawak (2010) "The importance of information security management in crisisPrevention in the company" Global Economic Crisis and Changes.

[13]. Tomasz Chajduga (2019) "Information security management in an individual documentomat project" World scientific News 122 pg 32-43

[14]. Yufei Yuan,Zhiling Tu (2014) " Critical Success Factors Analysis on EffectiveInformation Security Management: A Literature Review", Information Systems Security, Assurance, and Privacy Track (SIGSEC).