Journal of Theoretical and Applied Information Technology
20th September 2014. Vol. 67 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

EVALUATION OF EMPLOYEES AWARENESS AND USAGE OF INFORMATION SECURITY POLICY IN ORGANIZATIONS OF DEVELOPING COUNTRTIES: A STUDY OF FEDERAL INLAND REVENUE SERVICE, NIGERIA

[1]WADZANI A. GADZAMA, [2]JATAU ISAAC KATUKA, [3]YUSUF GAMBO, [4]ALIYU M. ABALI, [5]MUHAMMED JODA USMAN

[1]Department of Information Security, Faculty of Computing, Universiti Teknologi Malaysia.
[2]Department of Computer Science, Faculty of Computing, Universiti Teknologi Malaysia.
[3]Department of Computer Science, Adamawa State University Mubi, Nigeria.
[4]Department of Computer Science, Federal University Dutse, Nigeria
[5]Department of Mathematical Sciences, Bauchi State University Gadau, Nigeria.

E-mail: [1]ask4gadzama@gmail.com, [2]isaacjatau@gmail.com, [3]yusufu.gambo@gmail.com, [4]aliyuabali@gmail.com, [5]umjoda@gmail.com

ABSTRACT

Information security policy has become an integral part of today's organizational operations. It is a set of rules that guides computer resource users to ensure confidentiality, integrity and availability of organization information resources. Federal Inland Revenue Service of Nigeria is a government organization that is responsible for collecting revenues to the government. Due to its nature, it is concerned with how to protect and manage its information resource. This can only be achieved through implementation of an effective information security policy. This policy will help to ensure the confidentiality, integrity and availability of its information assets are protected. The purpose of the study is to find out the precise nature of existing information security policy and also to access the level of IT staffs awareness and usage of the policy in organizations of developing countries using Federal Inland Revenue service, Nigeria as a study area. Questionnaires were distributed which consist of both open and closed ended questions. The data collected were analyzed and presented. The study reveals that the IT staffs are aware of the existence and usage of the information security policy to the success of the organization. It was also revealed that the lack of adequate management support has affected the use of the policy. The study recommends that the management support in terms of staff training and awareness programs, continuous monitoring, enforcement and periodic review of the policy should be made to ensure the effectiveness of the organization information security policy.

Keywords: *Federal Inland Revenue, Service, Information Security Policy, Models, Information and Communication Technology.*

1 INTRODUCTION

In today's modern society, the need for information security in all part of our human endeavor is increasing day by day. This is as a result of the use of Information and Communication Technologies (ICT) in all faced of our life to improve how things are being done. During the recent years, both private and public organizations regard information security as a vital tool to protect the confidentiality and integrity of organizations. Information security has become an important element in today's organizational environment. Federal Inland Revenue Service (FIRS) of Nigeria information resources have become a major target for most attackers. These attackers are dynamic in nature as a result of our today's electronic business environment. The protection and management of the organization network has become a major

Journal of Theoretical and Applied Information Technology
20th September 2014. Vol. 67 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

priority. These protections can only be achieved through the use of standards and guidelines that will help towards defending of the present and future breaches of information security both within and outside the organization. Organizations do not need to wait for the attacks to occur before they can establish policies that will protect them.

Despite the efforts made by organizations to put security policy in place, many still do not have such information security policies in place. The few that has, their employees are not using it properly or are not even aware of its existence and are not using it at all while others do not have a well-planned and manage policy. This is as a result of lack of understanding of the security risk that are associated with the organization information assets or as a result of inadequate knowledge on how to properly manage the security of the entire enterprise resource. This can also be as a result of negligence to properly determine the extent to which those losses can affect the organization objectives and reputation. If security is compromised, it will result to loss of vital information and it will also give a very bad image to the organization. Many security challenges cannot be resolved through the use of technological devices such as routers, firewalls and intrusion detection system but through a good and well planned information security in place.

The lack of proper protection of organization information asset will compromise the entire organizational vision and mission. Information security policy ensures that the protection of information confidentiality, integrity, availability of organization information is not compromised. The proactive management of information security vulnerabilities, thread and risk refers to information security management [1]. To properly manage issues related to information confidentiality and integrity, there is a need to have an up to date information security policy in place. This is because a good security system in place will help limit the attacks both from within and outside the organization.

Organizations also required a conducive work environment that is safe and secure. This level of safety and security can only be provided through the use of control measures that will ensure confidentiality, data integrity and access availability. The most efficient and effective control measures that can protect organizations information asset is the use of information security policy [2]. Information security policy must be properly implemented before it can provide protection to organization information systems. Information security policy serves as the first level of defense against any threat that might exploit the vulnerability of any organization [3].

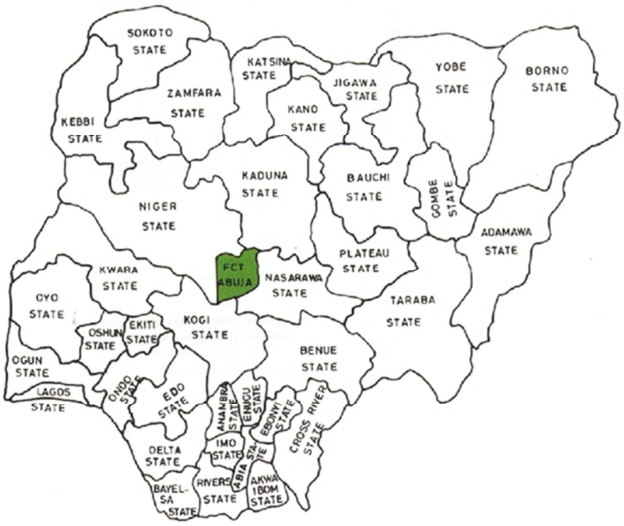

Figure 1: Nigerian Map

2 INFORMATION SECURITY POLICY

Information can come in different forms; verbal or written and in an electronic format [4]. It is an essential component for every organization's success; it plays a very critical role. The loss of information in an organization can cause a great damage in terms of its operation, finance and reputation [5]. Information is a key element of providing a quality service in an organization and it helps organization provides satisfactory services to their customers. Efficiency in terms of services can be fully obtained where relevant information is fully utilized [6]. The management and protection of information assets within organization required a formal document in making decisions; such document use for the decision support is called a policy [7];[8].

Information security policy is the most essential component in Information and Communication Technology (ICT) related security programs. Information security policy refers to as a set of rules and guidelines that computer resource users must follow and abide by to ensure that information resources confidentiality, integrity and availability is achieved [9]. Information security policy is an essential element to every organization's success. An organization can only appreciate its

Journal of Theoretical and Applied Information Technology
20th September 2014. Vol. 67 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

significances through proper implementation, constant monitoring and evaluation [10].

It is the responsibility of both the employers and employees to ensure that organization information assets are protected against unauthorized access, modification, deletion, and disclosure of any kind [11].

[12] Summarized the goals of the information security policy as follows;

i. Safeguarding the organization information assets including its employees by protecting its confidentiality, integrity and availability.
ii. To provide the protection mechanism that will safeguard the organization's information resources from abuse, theft and misuse or any kind of damage. And also to be accountable for organization information security.
iii. To inspire both the employee and their employers to maintain a suitable level of awareness, skills and knowledge to enable them to reduce the level of occurrence of incidence.
iv. To ensure continues operation of organizational activities in the event of incidence.

3 BACKGROUND OF FEDERAL INLAND REVENUE SERVICE, NIGERIA

The FIRS of Nigeria is a tax organization started as a Revenue Department of Anglophone department of West Africa which was later formed as a self-independent unit of income tax under the management of the commissioner of income tax. Many reforms took place before resulted in the FIRS of Nigeria of today. The head of the organization is usually appointed from among the directors of the finance ministry or an experienced person who has the necessary skills and knowledge of a private sector that can help government achieve their tax objectives. The FIRS have an autonomy given to them which has helped them improve the efficiency and effectiveness of their operations [13]. The FIRS have invested so much in the use of modern information and communication tools to improve the information security need of the organization assets. This investment in ICT has significantly improved the method of tax collection and processing of payments. It has reduced dubious activities among employees and also increases government revenue generation [13].

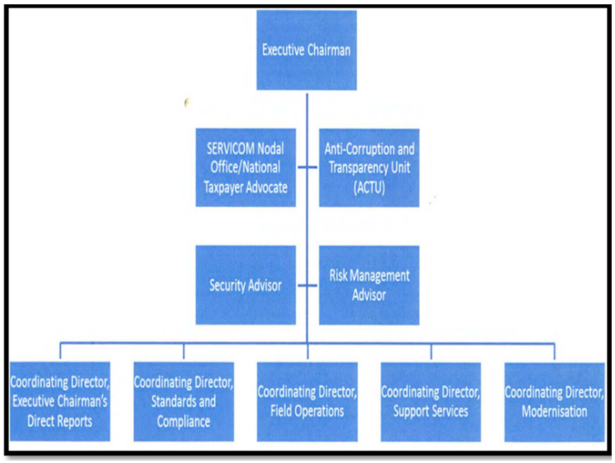

Figure 1: Firs Organization Structure [13]

3.1 The Need for Information Security Policy in FIRS

Information security policy is an objective statement that was established to guide the protection of an organization's information asset [14]. Therefore, it's necessary for any organization that wants to protect their information resources from unauthorized access and modification to see the need to establish and implements their organization's information security. The establishment and implementation of the security policy will reduce their vulnerabilities from any thread that might threaten the integrity and confidentiality of their information. The main essence of any policy is to provide a focus or guide for management of organizations who wish and determine to secure their information without violating their organization goals and objectives. [15] See information security policy as a blueprint that helps to provide a platform for organizational information systems by providing a secure working environment.

The Nigerian FIRS need information security policy due to large and sensitivity of information resources related to other enterprise, organization and business revenue records and collection details of revenues they work with every day. The data they collect and store is very important to the Nigeria as a nation because the revenue generated serve as an important factor in the country's economic development. This organization has at least one or more branches in each of the thirty six states in Nigeria. The importance of this organization makes it a potential target for other organizations, companies, and individuals who do

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

not want to pay their expected revenue to the government. These attacked may come from both within and outside the organization to modify the integrity of their records due to lack of payment of their revenue and the presence of an ineffective implementation of information security policy in place across the organization.

4 CLASSIFICATION OF INFORMATION SECURITY POLICY

Information Security Policy is categorized into three different types. This policy provides the managers with basis upon which they will establish their policies. Either of these policies can be found in most organizations [3].

4.1 A System-Specific Policy

It is a policy written for a specific system or device in an organization. It includes a set of guideline or procedures to be used when logging, using, configuring and maintaining a system. It focuses on specific issues related to a particular system or electronic device within the organization such as access control list that defines different levels of access for each authorized user [16].

4.2 Issue-Specific Information Security Policy (ISSP)

It addresses issues that are specific or related to technology-based system requirements or use [17]. It focuses on a use of specific or targeted technology. For instance, it may include issues such as the use of the Internet in the organization for personal use of the personnel. This policy may specify when workers are to use the internet to check their personal mails, chat with co-workers or friends, purchase things over the network. It may also specify what site should and should not be accessible and the period or days in a week it should be used.

4.3 An Enterprise Information Security Policy (EISP)

It is the formulation and integration of rules that define certain levels of permissions and access for different users in order to protect the information resources contained within the organization's network. It is also referred to as the general security policy [3]. It covers all information technology facilities of the organization not just on specific systems or issues related to any equipment within the organization. This type of Policy specifies the significance of the information security to the organization mission and objectives. It states all acceptable and unacceptable uses of organizational resources concerning Information security.

5 INFORMATION SECURITY POLICY MODELS

As a result in the increase of the global cybercrimes and the need for organizations to protect their information resource from thread, undoubtedly the most important and effective means of the control measures is the information security policy [10]. These models are as follows:

5.1 The Bull's Eye Model

The bull's eye Model is one of the models that insist on the use of policy in information security. In information security, bull's eye has been the most recognized Model. This model provides a holistic approach to organization solutions [3]. The goal of the bull's eye model is to protect the entire organization from any threat coming into the organization. Based on the bull's eye model, the information security policy is the first layer of defense in information security programs. In order to achieve the goal of information security (Confidentiality, integrity and availability) the importance of policy cannot be over emphasized. Security practice objectives and responsibility cannot be obtained without a clear definition of a policy in place [18].

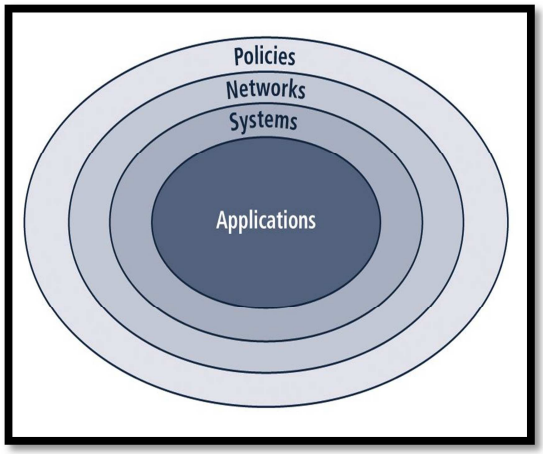

Figure 2: The Bull's Eye Model [3]

Journal of Theoretical and Applied Information Technology
20th September 2014. Vol. 67 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5.2 Repeatable Organizational Process Model

The model provides a strong practical representation of modern organization information security policy process [19]. This model was built based on the practical approach to many organization and information security professionals. Policy Retirement identifies that some policies are not actually needed during review and assessment, these policies can be retired. The double arrows in the process indicate that the policy can flow in either direction. The single arrow indicates the direction of flow and the dotted line indicates options that can be used. The semicircle on Policy awareness and training, monitoring and policy enforcement indicate that the phase has an ongoing process.

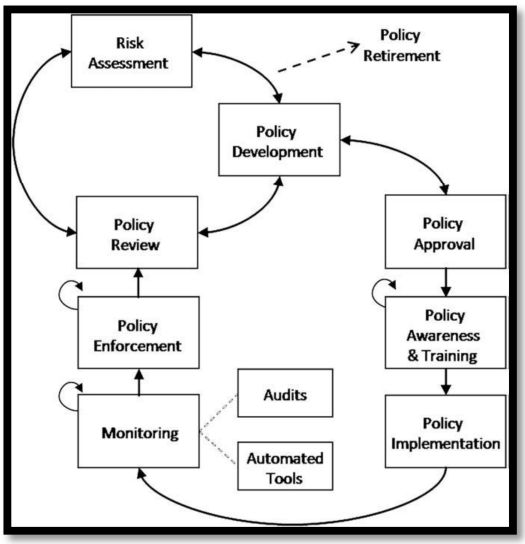

Figure 3: Information Security Policy as A Repeatable Organization Process [19]

5.3 Comprehensive Information Security Policy Process Model

This model provides information security governance structure with internal and external influence of the organization. It also provides a complete information security process model for information security officers within the organization [19].

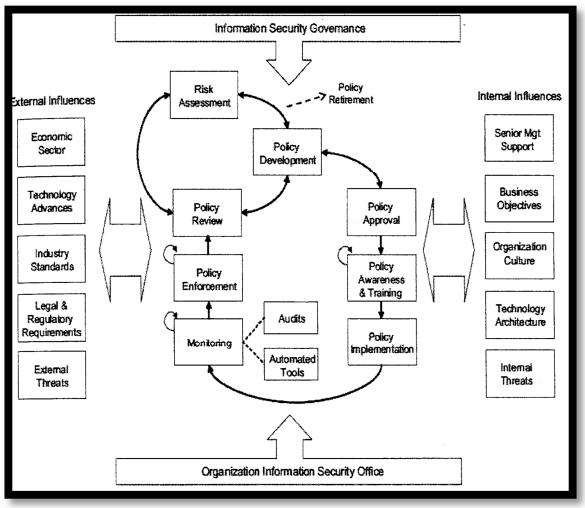

Figure 4: Comprehensive Information Security Policy process Model [19]

6 FRAMEWORKS FOR INFORMATION SECURITY POLICY

Organizations rely heavily on the use of information systems in their day to day operations. The need to protect the organization information system becomes a major challenge. The best way to protect the organization information system is through formulation of an effective information security policy. Many organizations have developed their policy while others have contracted the development of the policy to professionals based on the need of the organization [20]. The use of an information system in an organization has proven the reliability and effectiveness in their everyday operations. However, the use of information has also attracts security challenges that might exploit the vulnerability of the organization information system [21]. This security threat cannot be avoided.

The development and the implementation of an effective information security policy have become very necessary for the protection of an organization information system. [22] stated that the effectiveness of a security policy depends largely on the organizations management support, implementation control and continuous employees' awareness and evaluation of the policy. The confidentiality, integrity and availability of an organization's information assets can only be achieved through the formulation,

Journal of Theoretical and Applied Information Technology
20th September 2014. Vol. 67 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

development, implementation and the acceptance of an effective information security policy [23].

The significance of management support to produce an effective security policy through effective employees' awareness, training and evaluation is paramount [19]. However, despite the adoption and acceptance of information security policy to many organizations, the objective of the policy implementation has not been achieved. The reason for this is lack of proper management support and evaluation. For an organization's information security policy to be effective there is a need for constant monitoring, evaluation and enforcement. Another reason that may affect the effectiveness of an organization's information security policy is the inability of the policy security requirement to meet the organization objectives.

The security policy rules and guidelines should be centered to the organization employees [24]. As such, they developed a theoretical model on information system security policy that is based on the formulation, adoption and implementation of information system security policy.

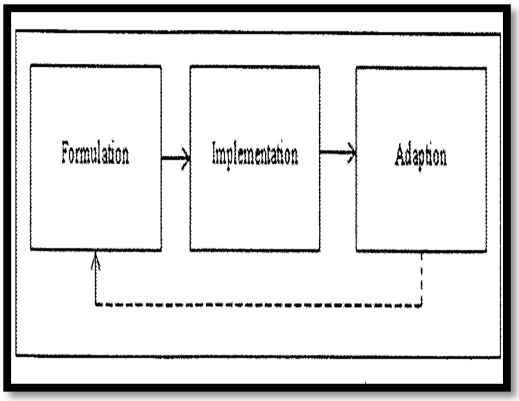

Figure 5: The Theoretical Model For Security Policy Application Process For An Effective Information Security [24]

Another theoretical framework model for an effective information security policy was created by [11]. The model consists of many elements. He insisted that those elements could be integrated to ensure an effective information security policy. The figure below shows effective information security policy elements.

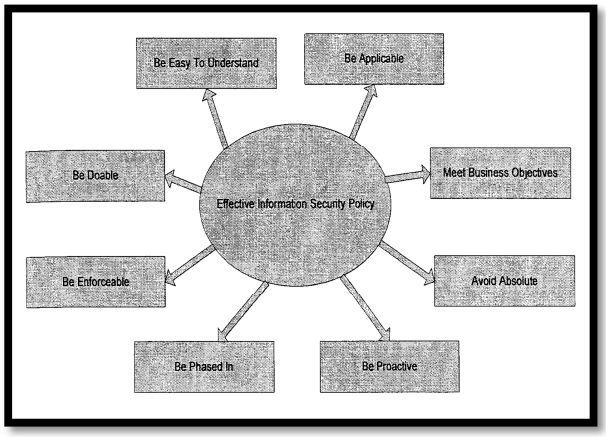

Figure 6: Elements Of Effective Information Security Policy [11]

A model for an effective information security was proposed [25]. This model was based on a consolidation study of information security system effectiveness. The model has key out the industry type, top management support and organization size. The information system security effectiveness has three dependable variables which include deterrent efforts, deterrent severity and preventive efforts. This model provides a security mechanism to prevent against misuse or unauthorized use of information assets by employees.

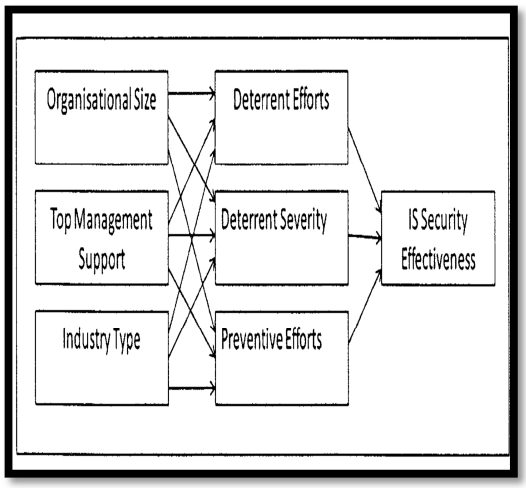

Figure 7: Model Of Information System Security Effectiveness [25]

Achieving the organization objective can be influenced through an effective information

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

security in place [10]. This is because the policy provides an effective guide to ensuring the security of an organization information system. The privacy of information assets plays a greater role in achieving organization's success. They developed a model for supporting activity for an effective information security policy. Supporting this activity plays a vital role in ensuring the effectiveness of an organization's information security policy. Below is the model.

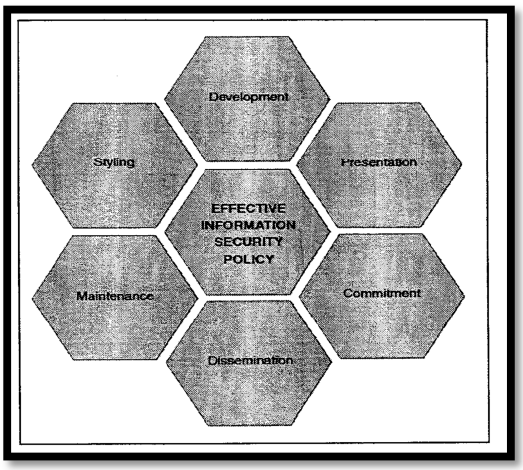

Figure 8: Supporting Activities For Effective Information Security Policy [10]

[26] Has developed a research model for an effective information security policy for user's perception of the institution of higher learning with reference to the University of Technology, Malaysia. The researcher insisted that an effective security model should be brief, precise, and concise and should state clearly the principle requirements to guide the policy principles. He also asserted that an effective communication and management of the information resource should be a continuous task. Below is the model developed by the researcher for effective information security policy.

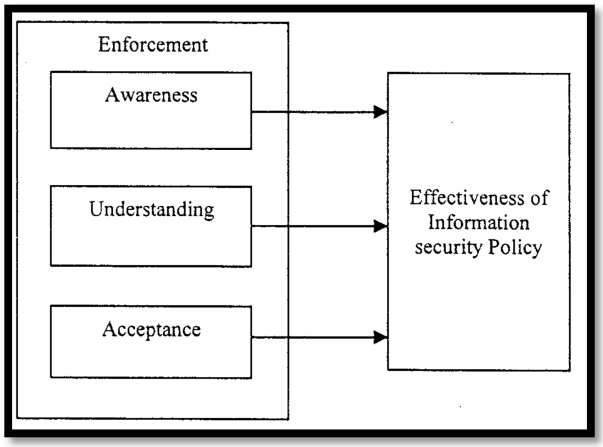

Figure 9: A Research Model For An Effective Information Security Model [26]

[27] Developed a research, model for awareness and acceptance analysis for an effective information security policy for Malaysian armed forces, cyber warfare division. The proposed model is shown below:

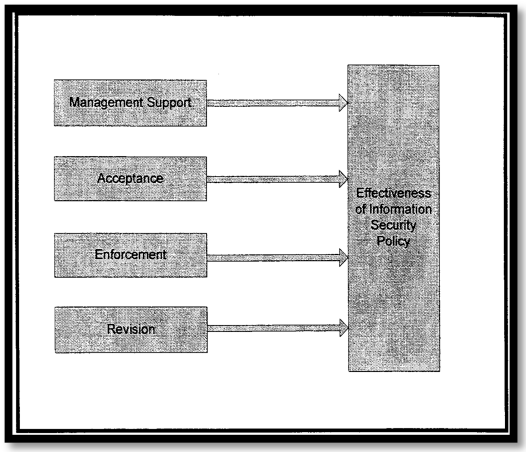

Figure 10: A Research Model For An Effective Information Security Model [27]

Thus, for an organization's information security policy to be effective, there are at least four prerequisite conditions [16].

i. Awareness: Employee's knowledge through an effective communication gives proper policy awareness.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ii. Skills: Possession of employees with job training gives good policy skills.
iii. Incentives: Penalties and rewards to adherence of the policy, influence employees use of the security policy
iv. Tools and Time: The use of the right tools and allocation of time are important to influence the use of the policy

To achieve an effective policy, the variables stated above must be used at any level. An effective policy depends on a good combination of employee behaviors and how they use the technology at their disposal. [28] stated that, there will not be any justification for the employees reluctance of the user security policy once there are properly communicated.

7 METHODOLOGY

7.1 Research Location

The research location is the main headquarters of FIRS, Nigeria Abuja because that is where the management decision and policies are created for the entire organization. The study of the main headquarters has given a desired result of the study.

7.2 Data Collection

Data collection is very important to any research work. It provides valuable information toward achieving the results of the study. The methods that were used in collecting data for this study include both the primary and secondary source.

a) Primary data

The primary source of data for this study is the questionnaire. The data was collected through the use of questionnaires from the FIRS, Nigeria Abuja. The questionnaire was used because it provides a quick means of obtaining employees respond/view on a wide range of subject. The use of a questionnaire has also helped in achieving an effective survey. The questionnaire consists of mostly closed ended questions and few open ended questions.

b) Secondary data

The secondary data for this study include books, journals, electronic resources and other related projects. Secondary data are very important because they provide the basis for literature review for this study and they helped a researcher with a broad knowledge of the topic of study.

7.3 Samples

A sample is a subset of the target population being studied. [29] For a sample to be accurate and represent the population, it must be large and a probability sample. The questionnaire that was generated from this study was given to thirty (30) IT staff of the FIRS of Nigeria to represent the population of the study area.

8 RESULTS AND DISCUSSIONS

8.1 Profile of Respondents

A total of 38 set of questionnaires were distributed to the information technology (IT) staff of the FIRS, Nigeria and out of the total number distributed only 30 were completely responded and collected from the survey.

Journal of Theoretical and Applied Information Technology
20th September 2014. Vol. 67 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

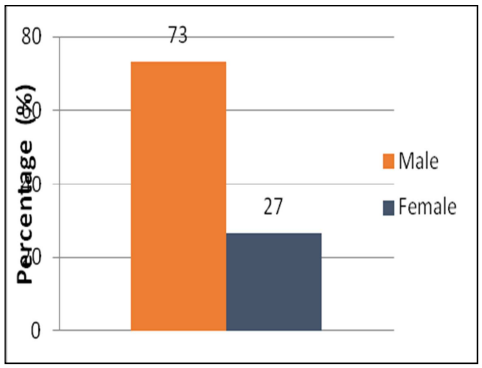

Figure 11: Gender

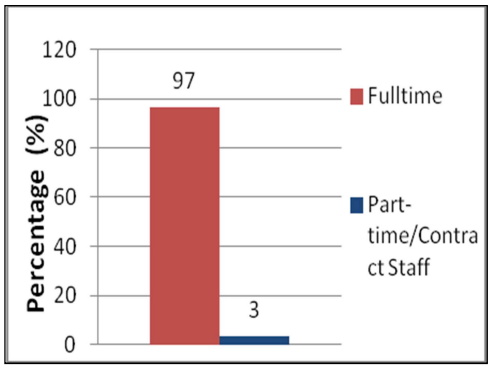

Figure 12: Type of Employment

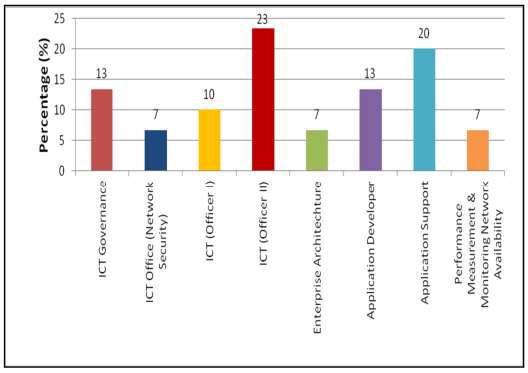

Figure 13: Job Title

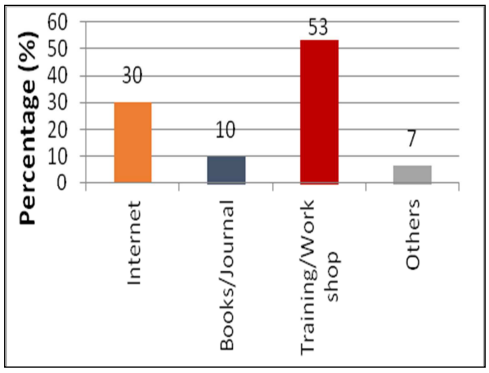

Figure 14: How IT Staff Came To Know About Security Policy In FIRS

From figure 11 above, it can be seen clearly that 73% of the IT staff are male and only 23% are female. This clearly shown that the FIRS prefer more men in their IT unit compare to female do to nature of their work. The Figure 12 above shown that 93% of the IT Staffs are Full time staff and only 3% are Part time /Contract staff. This indicates that the FIRS prefer permanent staff in the IT unit than the Part time/Contract due to its sensitive nature of work they do. From figure 13, it shows that ICT Officer II has the highest respondents with 23%, followed by application support with 20%. The least of the respondents consist of staff from the ICT Officer (Network Security), Enterprise Architecture and Performance measure and Monitoring Network Availability with 7% each. The outcome of this chart indicates that majority of the respondents of this questionnaires are ICT Office II and Application Developers. The Figure 14 shown that 30% of the respondents indicate that they first came to know about information security policy through the internet, 10% through Books/Journals while 7% through other means such as university education. The majority of them which consist of the 53% knew about information security policy through training and workshop. The outcome indicates that most of the IT staff know about security policy through on job training and work shop in FIRS.

8.2 Information Security Effectiveness in FIRS

The analysis under this section provides information about employees' awareness and knowledge of the units responsible for drafting and management of information security policy, its importance and how it has helped the FIRS towards achieving its security objectives.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

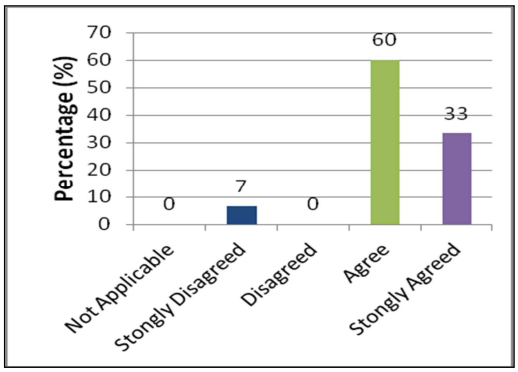

Figure 15: Awareness Of The Unit Responsible For Managing Security Polity In FIRS

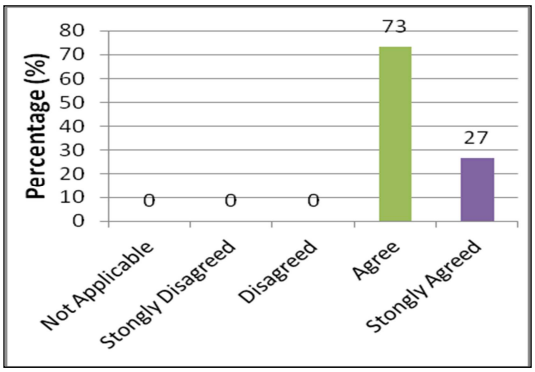

Figure 16: Benefits Of Information Security Policy

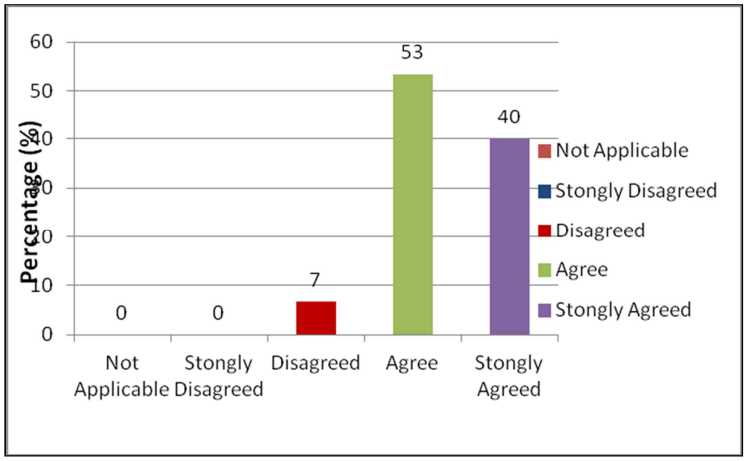

Figure 17: Role Of Information Security Policy In Achieving Security Objectives

As shown in Figure 15, more than three quarter 93% of the respondents are aware of the unit responsible for drafting and managing of information security policy within the FIRS. However, only 7% of the respondents strongly disagree. This outcome clearly indicates the level of commitment by the management to ensure that all their IT staffs are aware of the unit and officers responsible for creating and managing the organization information security policy. The Figure 16 above indicates that 100% of the respondents have either agreed or strongly agreed that they are aware of the importance and benefits of the information security policy. This result indicates that the IT staffs of the FIRS have a good knowledge of the importance of security policy in protecting the organization information assets. The study has shown that in the Figure 17 above that 93% of the respondents have either agree or strongly agreed that, they believe information security policy can help organizations in achieving their security objectives. However, 7% strongly disagree that the policy may not play any role in helping organizations achieve their security goals. Based on this responds, it can be concluded that information security policy is an integral document that ensure organization achieve its security objectives.

8.3 Management Support on the use of Information Security Policy

The Figures below in this section provide detail information of the staff awareness of the management approval, technical and financial support for the purchase and installation of the information security policy infrastructure in FIRS.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

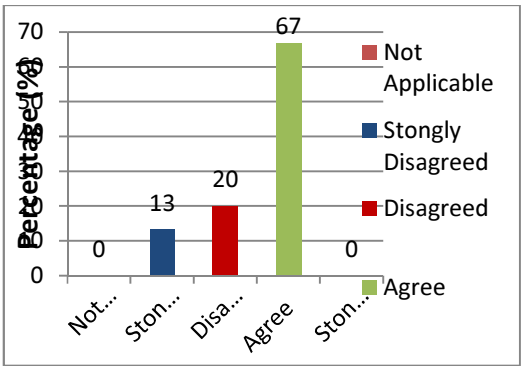

Figure 18: Management Approval Of Information

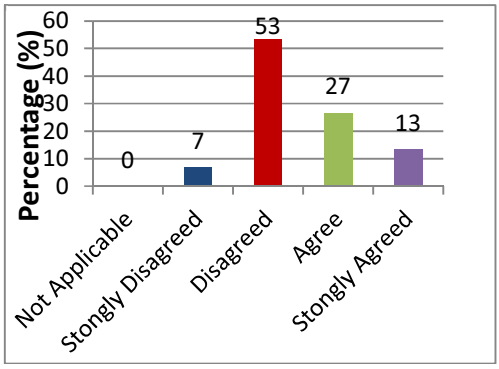

Figure 19: Management Support Of Information Security Policy Security Policy

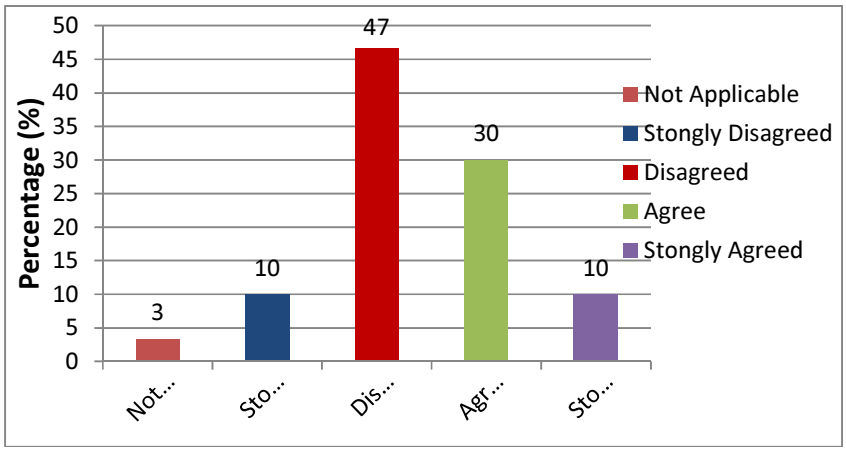

Figure 20: Management Support On The Purchase Of ICT Security Infrastructure

8.4 Employees Understanding and Acceptance of the use of Information Security Policy in FIRS

This section provides answers to questions on how IT staff in FIRS understood the aims and objectives of the policy, preventive measures needed to protect security thread, their knowledge with regards to reporting suspicious threats and their views with regards to other staff acceptance of the policy.

Journal of Theoretical and Applied Information Technology
20th September 2014. Vol. 67 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

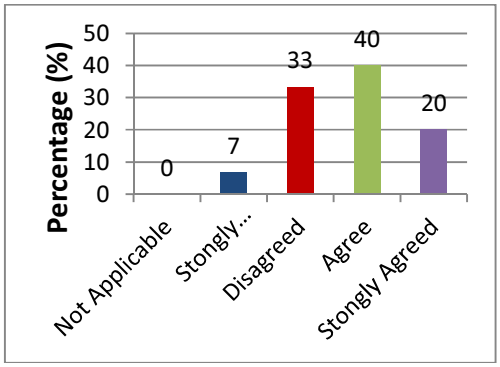

Figure 21: Employees Understanding Of The Goals Of Security Policy In FIRS

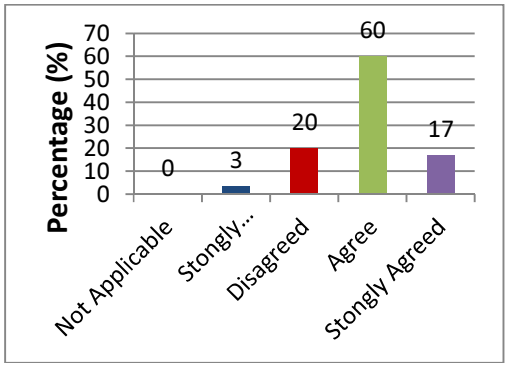

Figure 22: Preventive Measures Of Security Policy In FIRS

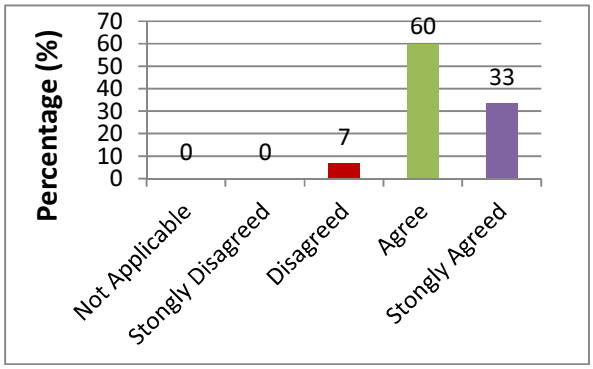

Figure 23: Need For Reporting Of Threats To The Unit In Charge Of Policy

The findings in Figure 21 clearly illustrate that majority of the respondents which are 60%, either agree or strongly agreed that they have clearly understood the aims and objectives of the security policy within the FIRS. However, only 40% does not clearly understand all its objectives. This result indicates that the management has not played a significant role in ensuring that that all its employees have fully understood the goals of using the policy within the FIRS. It can be seen in Figure 22 above that only 23% of the staff do not have adequate knowledge of the preventive security measures to protect the organization information assets and equipment. The vast majority which consists of the 77% are aware of the preventive measures to protect their respective resources. The organization must ensure that all of its IT staff should fully understand the preventive security measures to ensure that the organization is not liable to any threat. For organization to be safe, it must be able to prevent its information assets. The Figure 23 above, indicate 93% of the IT staff either agreed or strongly agreed that they are aware of the need to report any suspicious threats to the officers in charge or unit responsible on time to prevent successful attack. On the other hand only 7% disagreed with this claims. This outcome means that the management of FIRS are doing well enough in ensuring that their IT staff are aware of the need to report suspected security threats or issues to the personnel's or unit concern.

8.5 Information Security Monitoring in FIRS

Analysis in this part of the project gives an outcome on the staff knowledge on the management monitoring of the policy as well as response to reports regarding the use of the policy. It also shows employees knowledge of monitoring programs established by the management to manage security issues.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

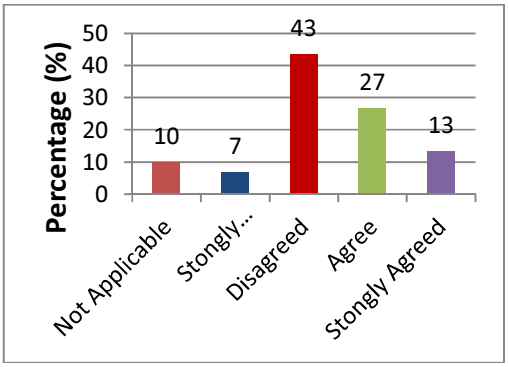

Figure 24: Monitoring Of Policy Application

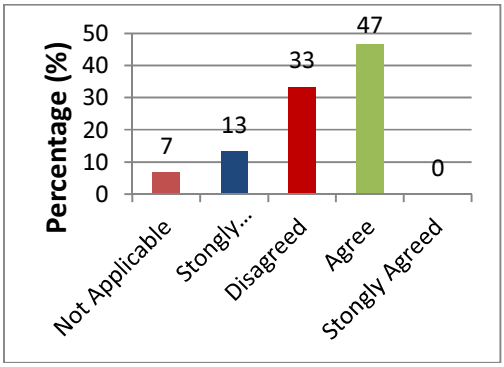

Figure 25: Response To Policy In FIRS Application In FIRS

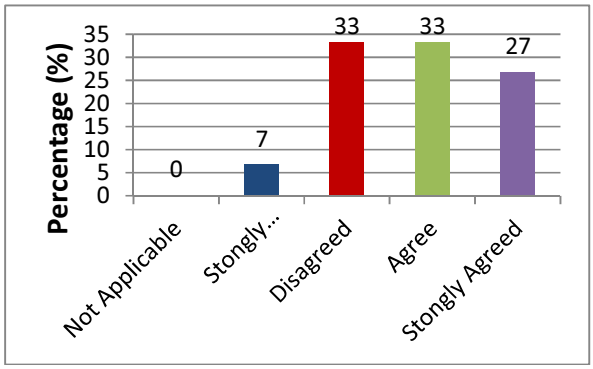

Figure 26: Policy Monitoring Programs In FIRS

Based on Figure 24 above, with respect to policy monitoring, only 40% of the respondents shows that they are aware and have either agreed or strongly agreed that the policy application is been monitored effectively periodically. 50% of the respondents either disagreed or strongly disagreed of having any knowledge about the monitoring of policy application. 10% are not aware of its existence. This outcome indicates that there is no any effective measure taking by the FIRS to ensure monitoring of the use of the policy by other staffs. Monitoring of security policy is very important towards ensuring its effectiveness. Based on the Figure 25 above, 47% of the respondents believed that there is adequate response to personnel's who have discovered and reported any security challenges regarding the use of policy in FIRS. On the other hand, 46% of the respondents have either disagreed or strongly disagreed with the claim above. However, 7% of the respondents do not have any idea on response to security issues by the management. This means that there is poor response to personnel's who have discover and complain any security challenges regarding the use of policy in FIRS. There is need to improve and have a prompt response time to ensure that staff can adequate use the policy effectively without any delay. As shown in the Figure 26 above, 60% of the respondents have agree or strongly agree while 40% either disagree or strongly disagreed about having knowledge on monitoring programs established by the management of FIRS to effectively monitored the security challenges in the organization. This result indicates that majority of the IT staffs are not fully aware of the applications use by the FIRS to monitor security issues that might affect the organization information assets. Its importance to ensure that a considerable number of staff have a very good knowledge of the monitoring program being used.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

8.6 The Enforcement of Security Policy in FIRS

The analysis below shows staff awareness and knowledge of any enforcement strategy by the management; penalties associated with the failure to comply with the policy and if there are any incentives use for the motivating of employees to comply with the use of the security policy.

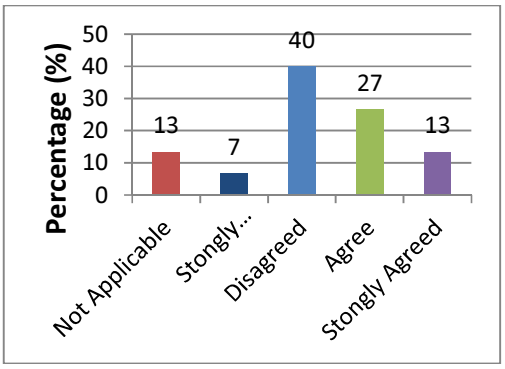

Figure 27: Policy Enforcement Strategy

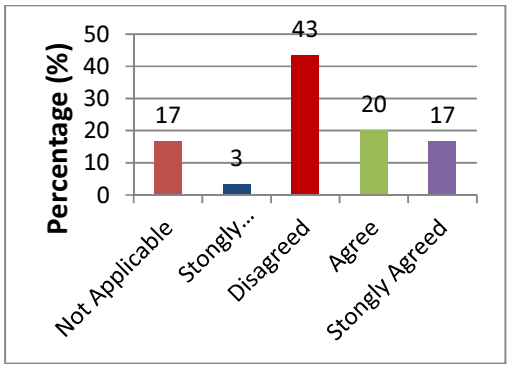

Figure 28: Penalties Associated

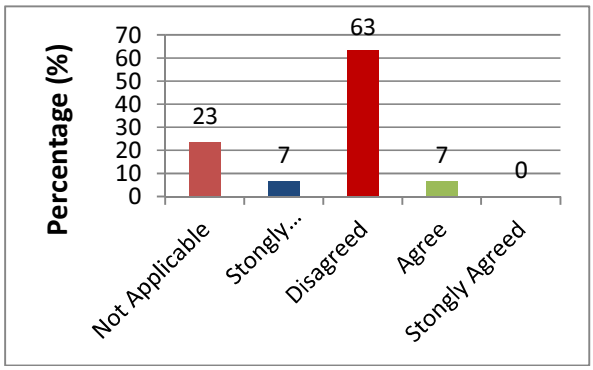

Figure 29: Incentives On The Use Of Policy In FIRS With Effective Use Of Policy

Figure 27 above, has clearly illustrated that 47% of the respondents have either disagree or strongly disagree and 13% are not sure on any enforcement strategy employed by the FIRS on the use of information security policy within the organization. Only 40% agreed or strongly agreed that enforcement strategy exist. This result indicates that there is no any effective means where policy application is been enforce on all the staff. To achieve effective security policy, there is a need to ensure strict compliance of the use of the policy through enforcement. The Figure 28 above portrayed that 46% of the respondents either disagree or strongly disagree of their awareness of any penalties employed by the organization that is associate with the failure to comply with the use of information security policy. Only 37% believe that some penalties exist. However, 17% are not sure if any penalty exists on the use of policy in FIRS. This response indicates that there is no any effective penalties involve in making sure that all staffs are conscious in ensuring the effective use of the policy in FIRS. From the Figure 29 above, only 7% agreed and 70% have either disagreed or strongly disagreed that there is no incentives in any form for motivating of employees who strictly comply with the use of security policy in FIRS. 23% do not have idea of any incentives that ever existed in FIRS with regards to policy usage. There is need to encourage staffs who works hard to ensure effective usage of the policy by given incentives over a period of time to encourage compliance. The outcome indicates that there is no

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

any incentives use by the FIRS for motivating and encouraging employees to comply with the use of the policy.

8.7 Review and Update of Information Security Policy in FIRS

This section analyzed data on whether the management updates its policy to meet the current security challenges, how security weaknesses are discovered and how they are being resolved. It also has shown how the staffs view the management use of ICT facilities and their views on the comprehensiveness of the organization policy.

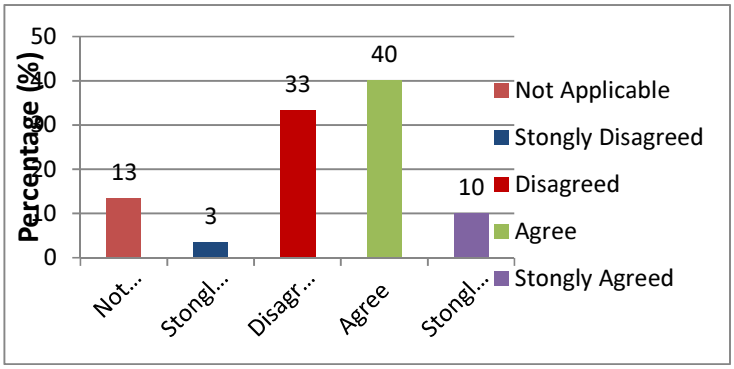

Figure 30: Information Security Policy Updates In FIRS

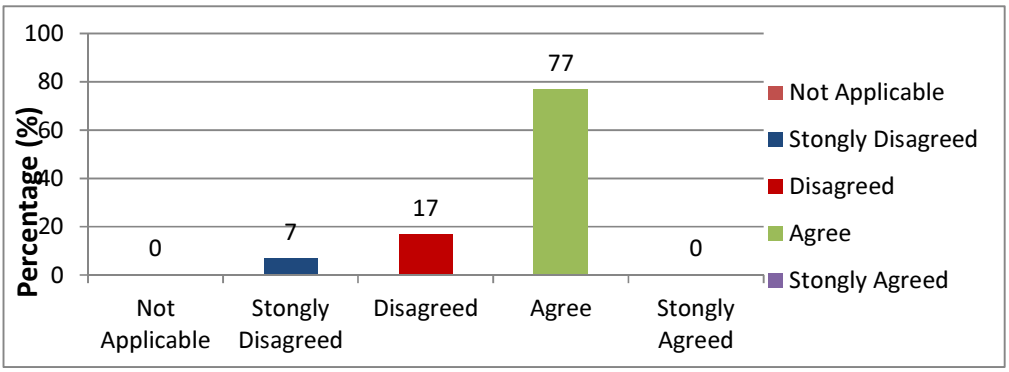

Figure 31: Respond To Security Challenges Discovered

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

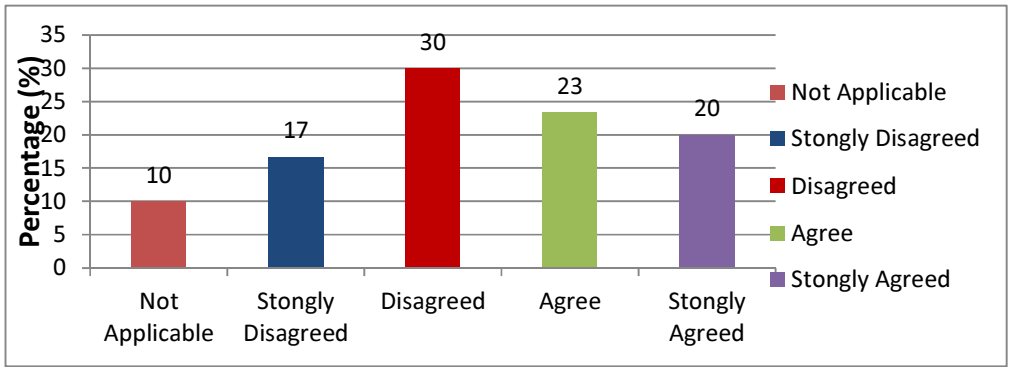

Figure 32: Use Of Current ICT Facilities In FIRS

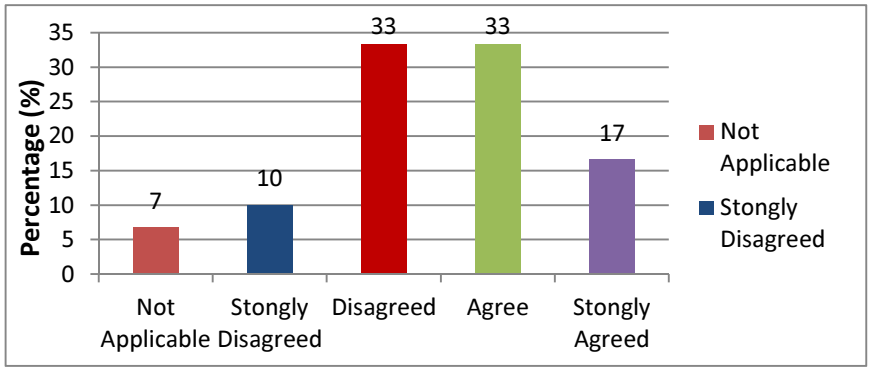

Figure 33: Comprehensiveness Of FIRS Information Security Policy

As clearly shown in Figure 30 above, 50% have either agreed or strongly agreed of their awareness of policy review and updates within the organization to meet the current security challenges. And 46% either disagreed or strongly disagreed that the current policy of FIRS has not been updated to meet the security challenges. 13% are not aware of existences of any update with regards to security policy in FIRS. The outcome indicates that only an average proportion of the staffs are convinced that such updates are taking place. There is need for the management to updates its policy over a given period of time to ensure that new challenges are covered in the policy. Figure 31 above clearly indicates that 77% of the respondent agreed that there is prompt respond by the management of FIRS for any security weakness or breach been discovered in the organization. Only 24% disagreed and strongly disagreed with such claim respectively. The results has shown that the management are doing well towards ensuring security weakness been discovered in FIRS are resolve in a good time. However, there is need to improve to ensure adequate respond in place. With respect to the use of current ICT facilities to ensure effective use of security policy, Figure 32 shows that 47% of the respondents have either disagreed or strongly disagreed that they are not aware of the management commitment with regards to purchase of currents ICT facilities that will help ensure effective security implementation. However, 43% respondents agreed with the use of up to date ICT infrastructure in FIRS while 10% of the respondents do not have idea on the facilities being used. This outcome indicates that the management must put strong effort to budget for the purchase of up to date ICT facilities that will improve the security of the organization. The Figure 33 above indicates that 50% of the respondents either agreed or strongly agreed that the FIRS information security policy is comprehensive. On the other hand, 43% disagreed that the policy is not standard. 7% of the respondents are not sure of its coverage in

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

terms of content, application and implementation. This result indicates that the staffs see the existing information security policy as partially comprehensive. The management must put so much effort in place to ensure that its security policy covers every organization information assets. This will ensure its effectiveness.

9 CONCLUSION AND RECOMMENDATION

Information security is becoming a great challenge to organization and business in our global world. The continuous use of information and communication technology tools is on the increase day by day. However, organizations who want to stand and succeed in their operations must develop and implement an effective policy in place that will guide and protect its confidentiality, integrity and availability. This can only be achieved through proper employee's awareness and usage of information security policy. This policy will provide a guide for a safe and secure working environment for an organization information assets and resources. It will also ensure its stability, confidence and competitive among other institutions. The study recommends some basic guidelines for an effective information security policy in FIRS based on the outcome of the study. The management of the FIRS should ensure that IT staffs have good information of the unit and officers in charge of handling policy related issues. There is need for management to ensure the IT staffs have up to date information on the importance and roles of the policy in achieving the organization objectives. Management should provide adequate support to policy usage and application within the organization to ensure its success. Employees should also be aware on the approval, updates and reviews with regards to policy related issues. As this will encourage them to improve their efforts since they are aware of the management approval and support. The management should ensure that policy monitoring is a continuous task to ensure that the goals of the policy are achieved. The government and the stakeholders should device a means to ensure that the policy monitoring is employed not only in FIRS but across all the Federal Government agencies in Nigeria.

REFERENCES:

[1] Kritzinger, E., Smith, E. (2008). Information Security Management: An Information Security Retrieval and Awareness Model for Industry. Computers & Security, Vol 27 (5-6) pp 224-231

[2] Knapp, K. J; Franklin Morris, R. and Marshall, T. E; et al. (2009): Information Security Policy: An organizational-level Process Model. In Computers &Security.

[3] Whiteman M.E. and Mattord H.J. (2010). Management of Information Security 3rd Ed. USA: Auebach publisher, Boca Rato pp. 117-152

[4] Muda M.Z., (2010). Awareness and Acceptance Analysis of Information Security Policy in Malaysian Air Force. Master of Computer Science (Information Security), Universiti Teknologi Malaysia.

[5] Hone, K. (2004). The Information Security Policy — An Important Information Security Management Control. (Degree Dissertation, Rank Afrikaans University, 2004). Dissertation of Mcom (Informatic), Faculty of Economic and Management Science.

[6] Sharif, H., (2009). User's Perception of the Information Security Policy at Universiti Teknologi Malaysia. Master of Computer Science (Information Security), Universiti Teknologi Malaysia.

[7] Peltier,T. R, Peltier, J. and Blacklay (2005). Information Security Fundamentals,Auerbach Publications, Boca Raton, Florida.

[8] Tudor, J.K. (2001). Information security architecture: An integrated approach to security in the organization. CRC Press LLC. ISBN 0-8493-9988-2

[9] Ragged B.G. (2010). Information Security Management: Concept and Practice.Auerbach Publications, Boca Raton, Florida.

[10] Hones one, K. & Eloff, J.H.P., (2002). Makes an Effective Information SecurityPolicy? Network Security, Volume 6, pp. 14-16.

[11] Peltier, T. R. (2004), Information Security Policies, Procedures, and Standards - Guidelines for Effective Information Security Management, Auerbach Publications, Boca Raton, Florida.

[12] ISP (2009). Information Security Policy Objectives. Information Security Policy World. The Security Policies & Standards Group, London. Available: http :I/www. inforrnationsecurity-policies-afld-standardS.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

com/obi ective.html. [Accessed on January 15, 2013]

[13] FIRS (2013). Federal Inland Revenue Service, Nigeria Publications. Available: http://www.firs.gov.ng/About-Us/What-FIRS-Does.aspx [Accessed on January20, 2013]

[14] Gaston, S.J. (1996). Information Security: Strategies for Successful Management. Toronto: CICA.

[15] Von Solms, B., and von Solms, R. (2004), The 10 deadly Sins of Information Security Management, Computers and Security, Volume 23, pp.371-376

[16] Marcinkowski, S. and Stanton, J., (2003). Motivational Aspects of Information Security Policies. In Systems, Man and Cybernetics, 2003. IEEE International Conference on. pp. 2527-2532 vol.3.

[17] Peltier, T. R. (2004), Information Security Policies, Procedures, and Standards - Guidelines for Effective Information Security Management, Auerbach Publications, Boca Raton, Florida.

[18] Higgins,H.N.(1999). Corporate System Security: Towards an Integrated Management Approach. Information Management and Computer Security, 7(5), pp. 217-222.

[19] Knapp, K. J; Franklin Morris, R. and Marshall, T. E; et al. (2009): Information Security Policy: An organizational-level Process Model. In Computers &Security.

[20] Stephen P. B. (1996). Theoretical Framework. Available: http://www.analytictech.com/mb313/elements.html. [Accessed on March 3, 2013]

[21] (ISO). ISO/IEC 27002 (2005), Information Technology - Code of Practice for Information Security Management, International Organization for Standardization

[22] Karyda, M., Kiountouzis, E., and Kokolakis, S. (2005), Information systems security policies: a contextual perspective, Computers and Security, Volume 24,pp. 246-260.

[23] Yip,F., Ray, P. and Paramesh, N (2006). Enforcing Business Rules and Information Security Policy Through Compliance Audits; XISSF- A Compliance Specification Mechanism In: The first IEEE/IFIP International Workshop on Business Driven IT Management (BDIM, 2006)- Information Technology Management from Business Perspective, pp, 81,90

[24] Maria, K., Evangelos, K., and Spyros, K. (2004). Information systems security policies: a contextual perspective.Computers & Security Volume 24, Issue 3, May 2005, pp 246-260.

[25] Kankanhalli, A., Teo, H.H, Tan, B.C.Y., and Wei, K.K. (2003). An integrative study of information systems security effectiveness. International Journal of Information Management (2003). ISSN 0268-40 12.

[26] Sharif, H., (2009). User's Perception of the Information Security Policy at Universiti Teknologi Malaysia. Master of Computer Science (Information Security), Universiti Teknologi Malaysia.

[27] Muda M.Z., 2010. Awareness and Acceptance Analysis of Information Security Policy in Malaysian Air Force. Master of Computer Science (Information Security), Universiti Teknologi Malaysia.

[28] Saleh, M.S., Alrabiah, A., and Sand, H. B. (2007). Using ISO 17799; 2005 Information Security Management: A STOPE View With Six Sigma Approach. International Journal of Network Management, 17(1), pp. 85-97.

[29] Jen S.U. (2012). Fundamentals of Research Methodology. 3rd ed. Yola-Nigeria. Paraclete Publisher pp. 53-74