International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 7, July - 2014

Conceptualized Framework for Evaluating a Network Security Policy

Enoch Ainoo mbir
Research Scholar
Sikkim Manipal University
Accra, Ghana

Kamal Kant Hiran
Head, Department of IT
Sikkim Manipal University
Accra, Ghana

***Abstract* - A security policy is a set of rules and practices prescribing how important information is managed, protected, distributed, and also expresses the precise security level by defining which security methods are to be performed. Network security rests on confidentiality, integrity, and availability which recognizes the threats and clarifies the requirements to provide a secure network to detect and prevents attacks and enables recovery as well.**

The motivation behind this research is that it seeks to formulate protocols and standards for the design and implementation of a network security policy by the creation of a survey which comprises a series of questions. The survey was conducted at Central University College (CUC) and questionnaires distributed to all members of staff who have access to electronic information and the network and also define the assets that will be protected by the network security policy. Network security can cover a wide range of issues from physical security to personnel security as well as procedural security.

Keywords— Security Policy, Security threats

I. INTRODUCTION

Network security focuses on confidentiality, integrity and availability which recognizes the threats and clarifies the requirements to provide a secure network to detect and prevents attacks and enables recovery as well. A security policy is a set of rules and practices prescribing how important information is managed, protected, distributed and also expresses the precise security level by defining which security methods are to be performed [1] (Michael, 2005). It is an important part to protecting information assets in a network environment and plays a major role in defining the design of a network. The security policy is a base for the specifications of a system and provides the baseline for evaluating a system. A system provides trust by executing the security policy and also deals with the relationship between subjects and objects [2] (Matt, 2005).

II. NETWORK SECURITY, POLICIES AND STANDARDS

Before examining various types of network security policies, it is important to understand the relation between policies, standards and practices. Security policies, standards and procedures fit into the following hierarchy. Policy: It is a high level statement of an institution or a company's goals and objectives and general means for their attainment for a specified subject area.

Policy Content Consideration: A policy document should be approved by management published and communicated as appropriate to the employees. It should state management commitment and set out institutional approach to managing network security. The content should include the following contents [9].

- A definition of network security, its overall objectives, scope and importance of security.
- A statement of management intention, supporting the goals and principles of network security.
- A brief explanation of specific security policies, standards and compliance requirements including compliance with legislative and contractual requirements as well as security awareness and education requirements.
- Satisfy legal and contractual requirements for security.
- Provide enforcement and recovery guideline (including insurance coverage) for instances when a compromise of security is detected.
- Protect and provide a secure and safe work environment for its employees.

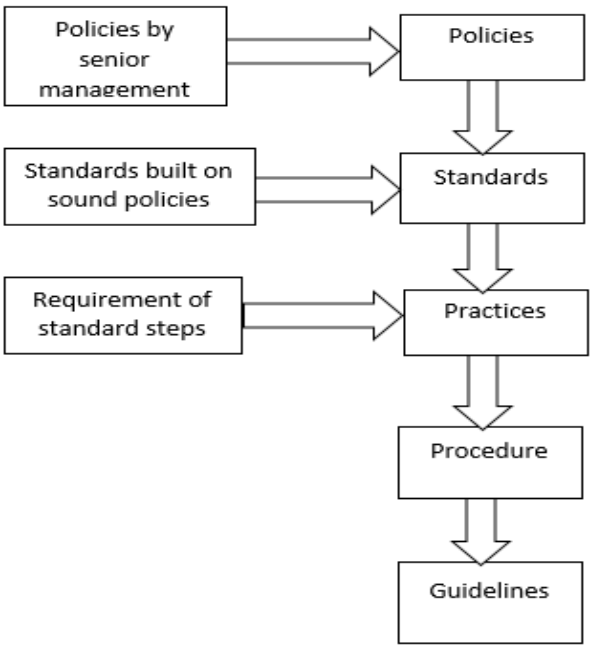

Fig. 1. Policies, standards and practices.

Policy is a plan of action to convey instructions issued by senior management to its concern staff which performs duties on the behalf of the institution while standards are the detailed statements which specify what must be done to comply the policy whereas Practices, Procedures and Guidelines effectively explains how to implement the policy.

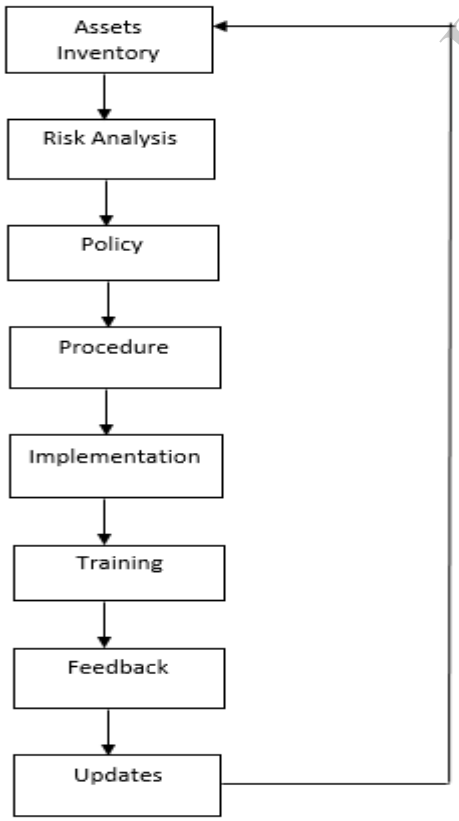

Fig. 2. Policy design life cycle

A. Assets Inventory:

An asset is a resource of an institution that is being protected. Asset can be logical such as web site, information or data or asset could be physical like a person, computer system or other tangible object. Particularly, network or information assets are the focus of security efforts and are what is being protected. This is why inventory of assets is needed to identify the risk associated with related assets.

B. Risk Analysis

In network security, risk could be the probability of a threat to the system, the probability of vulnerability being discovered or probability of equipment or software malfunctions. Risk analysis can be the risk which can be measured in terms of qualitative or quantitative terms.

C. Policy

Once the risk is identified, institutions objective is to protect those assets so as to reduce the risk. Policy is high level statement of organization for attainment towards protection of information assets of organization.

D. Procedure

As discussed earlier, procedures are focused on how the policy will be actually implemented in operating environment.

E. Implementation

This is actual execution of a policy based on certain standards and guidelines followed by the institution.

F. Training

This involves providing awareness to the members of the institution with detailed information and hands on instruction to prepare them to perform their duties securely.

G. Feedback

After implementation is in process, the opinions of the users are taken about the procedures and standards applicable to the policy. With appropriate opinions the policy can be further modified or updated.

H. Update

This is the last phase of the policy design life cycle where changes in the existing policy are reviewed and implemented in the specific policy.

III. ANALYSIS

In this chapter, data gathered from the research is presented by tables and pie charts. Analysis was undertaken to draw inferences in questionnaires distributed. The research was based on the total of thirty-five (35) human population of central university. Out of the distributed (35) questionnaires, nineteen (19) were retrieved of which the following percentages and numbers were obtained from the analysis of the questionnaires.

TABLE I. TOTAL DISTRIBUTED QUESTIONNAIRE

Categories of Ques	Quantity of Ques	Respondent	Non - Respondent	% of Respondent
Physical Security	35	19	16	54%
Program Change	35	19	16	54%
Backup Recovery	35	19	16	54%
Disaster Recovery	35	19	16	54%
Computer Operation Controls	35	19	16	54%
Network Control	35	19	16	54%
Personal Computer	35	19	16	54%
Internet Controls	35	19	16	54%

Nineteen (19) responded to "physical security questions", non -respondent is sixteen, percentage of respondent is 54%, percentage of non -respondent is 46%, total number of people who answered "yes" are seventeen (17), total number of people who answered "no" are two(2), percentage of people who answered "yes" is 89% and percentage of people who answered "no" is 11%. Nineteen (19) responded to "program change questions", non -respondent are sixteen (16), percentage of respondent is 54%, percentage of non -respondent is 46%, total number of people who answered "yes" are eighteen (18), total number of people who answered "no" is one(1), percentage of people who answered "yes" is 94% and percentage of people who answered "no" is 5%. Nineteen (19) responded to "Back up recovery questions", non -respondent are sixteen (16), percentage of respondent is 54%, percentage of non -respondent is 46%, total number of people who answered "yes" are sixteen (16), total number of people who answered "no" are three (3), percentage of people who answered "yes" is 84% and percentage of people who answered "no" is 16%. Nineteen (19) responded to "Disaster recovery questions", non -respondent are sixteen (16), percentage of respondent is 54%, percentage of non -respondent is 46%, total number of people who answered "yes" are fifteen (15), total number of people who answered "no" are (4), percentage of people who answered "yes" is 78% and percentage of people who answered "no" is 21%. Nineteen (19) responded to "Computer operation control questions", non –respondent are sixteen, percentage of respondent is 54%, percentage of non -respondent is 46%, total number of people who answered "yes" are two (2), total number of people who answered "no" are seventeen (17), percentage of people who answered "yes" is 11% and percentage of people who answered "no" is 89%. Nineteen (19) responded to "Network security questions", non -respondent is sixteen (16), percentage of respondent is 54%, percentage of non -respondent is 46%, total number of people who answered "yes" are ten (10), total number of people who answered "no" are (9), percentage of people who answered "yes" is 52% and percentage of people who answered "no" is 47%. Nineteen (19) responded to "personal computer usage questions", non –respondent are sixteen (16), percentage of respondent is 54%, percentage of non -respondent is 46%, total number of people who answered "yes" are fourteen (14), total number of people who answered "no" are five (5), percentage of people who answered "yes" is 74% and percentage of people who answered "no" is 26%. Nineteen (19) responded to "Internet control questions", non –respondents are sixteen (16), percentage of respondent is 54%, percentage of non -respondent is 46%, total number of people who answered "yes" are seventeen (17), total number of people who answered "no" are two (2), percentage of people who answered "yes" is 89% and percentage of people who answered "no" is 11%.

TABLE II. CONTINUATION OF TOTAL DISTRIBUTED QUESTIONNAIRE

% of non-respondent	Yes	No	% of Yes	% of No
46%	17	2	89%	11%
46%	18	1	94%	5%
46%	16	3	84%	16%
46%	15	4	78%	21%
46%	2	17	11%	89%
46%	9	10	47%	52%
46%	14	5	74%	26%
46%	17	2	89%	11%

Table 1, 2 and Fig 1 shows a summary response of the total distributed questionnaires used under this research paper.

EQUATIONS USED TO CALCULATE PERCENTAGES

- Quantity of questionnaires=∞
- Respondent=β
- Non respondent=α
- Yes=μ
- No=π

CALCULATION FOR "RESPONDENT" AND "NON RESPONDENT"

$$\beta/\infty*100 \textbf{ or } \alpha/\infty*100 \quad (1)$$

PERCENTAGE CALCULATION FOR "YES" OR "NO"

$$\mu/\beta*100 \textbf{ or } \pi/\beta*100 \quad (2)$$

The following equations were used to derive at the various percentages and calculation of the respondents and non-respondents.

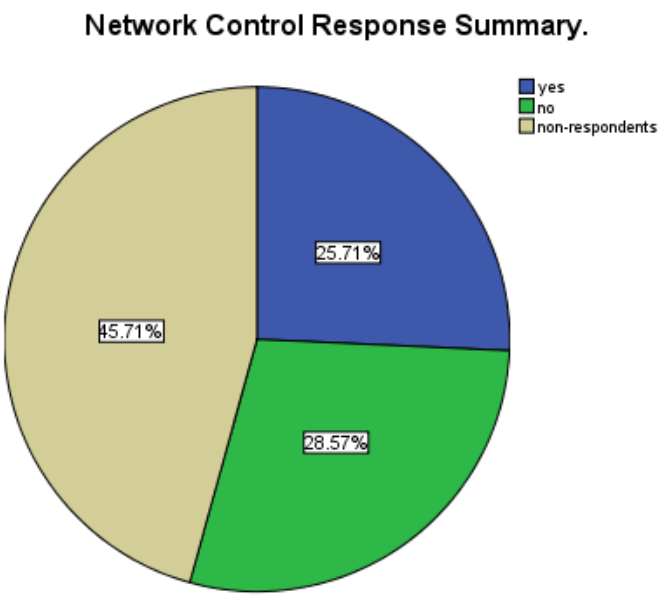

Fig. 3. Network control response summary questionnaire.

From Fig 1, inference can be deduced that only forty seven (25.71%) of a good network security policy is implemented at central university college whiles fifty two (28.57%) of a good and secure network policy is ignored. (45.71%) represent no response in relation to the distributed questionnaires of network security control. Summary of Fig 3 indicate that the network security policy of central university college have to be reviewed to contribute a good network security control.

ACKNOWLEDGMENT

I am very grateful to the Almighty for giving me the opportunity, strength and the intellect to undertake this project. My sincere gratitude goes to Central University College for giving me this opportunity to come out with this piece of work. I am also acknowledging Mr. Alwyn. Amarteifio Head of department Central University College (IT), thank you for your constructive criticism, suggestion, advice, your time and effort spent to supervise this work. To, Mrs. Olivia Kissi Mbir, my sincere gratitude goes to you for the encouragement and final proof reading. You are really a strong pillar.

REFERENCES

[1] Michael E. Whitman and Herbert J. Mattord, "Principle of Information Security", 2nd edition, Thomson Course Technology, February 2005.

[2] Matt Bishop, "Introduction to Computer Security", Addison-Wesley, December 2005.

[3] Dowd, P.W.; McHenry, J.T, "Network security: it's time to take it seriously," Computer, vol.31, no.9, pp.24-28Dieter Gollmann, "Computer Security", Wiley, Sep 1998

[4] James Michael Stewart, Mike Chapple, 2003. "CISSP:Certified Information System Security Professional", 2nd edition, Sybex Inc.

[5] Brad Woodberg, Rob Cameron June 2013.A Comprehensive Guide to Security Services on the SRX Series.

[6] Steve Mallard, "Understanding the Impact and Solutions of Computer and Network Security in today's World", June 2007.

[7] Thomas R.Peltier, Information Security Policies, Procedures and Standards, Guidelines for Effective Information Security Management, Auerbach Publications, Pg. [31-32], April 2002.

[8] SecurityOverview,"www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/security-guide/ch-sgs-ov.html.

[9] Charles P. Pfleeger, Shari Lawrence Pfleeger, "Security in Computing", Prentice Hall PTR (United States of America), November 2002.

[10] Rick Lehtinen, "Computer Security Basics", O'Reilly (United States of America), August 2006.

[11] David Salomon, "Foundations of Computer Security", Springer- Verlag (London), May 2006.

[12] Matt Bishop, Computer Security: Art and Science, Addison Wesley (United States of America), January 2002.

[13] Ralph Kimball, "the data warehouse toolkit", Wiley India Pvt. Limite, Jan 1,2004.

[14] Matt Bishop, 2002, Computer Security: Art and Science, Addison Wesley (United States of America).

[15] Ralph Kimball, Jan 1, 2004, the data warehouse toolkit, Wiley India Pvt. Limited.

[16] C.C Nwachukwu(1988):Management Theory and Practice, Africana Publishers.

[17] Heinnemann, J (1994): Business Studies, Shaw Publishing, London.

[18] Stoner et al (1995): Management 6th Ed. Addison-Wesley Publishing Company New York.

[19] Lynch (2001): Managing people, published by Foulks Lynch Ltd.

[20] Andrew J. Dubrin (2006): Essentials of Management 7th edition.