INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

THE EFFECTS OF FIREWALL ON COST EFFICIENCY AMONG SELECTED BUSINESS ORGANIZATIONS IN NIGERIA

[1]DAWODU BAMIDELE FRIDAY (M.Sc), [2]OSONDU MARY C (M.SL)
[1]bamidele4dawodu@gmail.com TEL: 08038174792
[2]*ogamc@yahoo.com* TEL: 07035798056

[1]DEPARTMENT OF INFORMATION TECHNOLOGY/FEDERAL UNIVERSITY OF TECHNOLOGY, IMO STATE
[2]THE LIBRARY (ICT UNIT)/FEDERAL UNIVERSITY OF TECHNOLOGY, IMO STATE

ABSTRACT

This work is intended to study the effects of firewalls on cost efficiency among selected business organizations in Nigeria; the researcher sets out to study the different aspects or areas that should be considered when deploying firewall security systems in business organizations. These aspects of security can be stated as follows: hardware security aspect, software security aspect, database security aspect, network security aspect. In doing this, the researcher formed and distributed questionnaires to respondents. Some results were used in this analysis, as some respondents did not return theirs while others were inaccurate. The valid results were analyzed using multiple regression, and it was discovered from the analysis, that the whole aspects of firewall security offers cost efficiency to business organizations. Then individually it was discovered that database security aspect and network security aspects have significant effect on cost efficiency among business organizations, while hardware security aspect and software security aspects do not have significant effect on cost efficiency. From the analysis business organizations are also advised to invest more in hardware and software security to improve cost efficiency among business organizations.

Keywords: Firewalls, Security, Analysis, Business, Organization, cost efficiency

1. Introduction

Computer network is the discipline concerned with communication involving computer systems and devices. The purposes of networking are for the exchange and sharing of data resources. Within a network large volume of data can be exchanged through both short and long-range connections. Likewise computer resources such as hardware (printer, scanner etc.) and software can be remotely shared among network hosts. With increased reliance on computer network, calls for serious monitoring of the traffic in and out of the system network [1][6][5][7][8]. Today there are tools for probing the movement of data or information in and out of networks that has given birth to network security threat [2][3][4]. The worst situation occurs when the internal computer network is made to connect

with the internet, because of the openness of the internet; every corporate network connected to it is vulnerable to attack. Hackers on the internet could break into the network and do harm in a number of ways; they can steal and cause damages to important data, damages to individuals computers and the entire network, use of internal network resources. Due to some of these security threats, there is the need to build a defensive mechanism that ensures that hackers and their likes are not allowed into the network. A Firewall then can be said to be a software or hardware device installed at the point where network connection enters an internal network [18][19][20][21][22][23]

Sets of rules are applied to control the type of networking traffic flowing in and out of the system. Firewall security systems are designed to stop unwanted or suspected traffics from flowing into the internal network. This would ensure that hackers have no access to the internal network. Thus, the basic function of a firewall is to regulate the flow of traffic between computer networks of different trust levels. The Internet is a zone of no trust, unlike an intranet which is an internal network with a good level of trust. Due to the expansion of corporate enterprise network to include Internet connections, this has introduced dangers to the internal (organizational) network [1][12][8][9[14][10]. A firewall in a computer network performs a role that is very similar to that of a firewall in a building. Just as a firewall, made out of concrete protects one part of a building, a firewall in a network ensures that if something bad happens on one side of the firewall, computers on the other side won't be affected. Unlike a building firewall, which protects against a very specific threat (fire), a network firewall has to protect against many different kinds of threats and thereby reducing the cost of running a computer network which encompasses different levels of computers and devices [6][11][12][13]. Firewalls can provide a cost-efficient means of protecting a local system or network of systems from network-based security threats while at the same time affording access to the outside world via wide area networks and the Internet. With these ideas in mind, a cost-efficient way of improving security solution was implemented and as such all the inbound and outbound traffic pass through the firewall when installed and fully implemented on a network [14][15][16]. The firewall in turn determines which traffic should be allowed in or out of the network. This software or hardware apart from preventing unauthorized access to the network also prevents virus, worms, and Trojan horse attack. Therefore, this study will carry out an analysis on the effects of firewall on cost efficiency on networked systems and also, how networks can be monitored in order to prevent unauthorized access to internal networks[20][21][22][23].

2. STATEMENT OF THE PROBLEM

The absence of firewall security has generally resulted to a huge loss on the side of many business organizations that have computer networks established in their various fields of work. The sensitivity of firewall security systems has enhanced network security and thereby reduced a great deal of cost to many organizations. Firewall sensitivity in computer networks and devices contributes to a higher return on investment among business organizations and as such reduce the expense of cost in running networks.

A compromised computer affects all the other computers that are connected to the same network [6][7][8]. The speed and reliability of a network can be affected, because compromised computers may cause large amounts of network traffic and often attack computers on the network. Many organizations greatly suffer threats from hackers, who wilfully gain easy entrance into a network, thereby causing havoc to the network and its environment. Viruses and Worms are among the biggest Cyber Security threats. They spread by infecting insecure computers that, in turn, infect other insecure computers. For restrictions to different levels of insecurity, incoming and outgoing e-mails should be monitored for suspicious attachments. Some attachments, such as .exe or .com files, are not allowed to be received in e-mail from the internet because they are frequently used in spreading viruses. Infected and compromised computers may have their network access disabled to isolate network problems. This is done to keep the entirety of the network secure while infected computers are repaired. To prevent and eliminate cyber attacks such as financial losses, leakages of business concepts, data and strategies, the use of a firewall technology system should be greatly encouraged in combination with regular security updates for our operating system and virus-definition updates. This piece of work will be able to study the effects of firewall on cost efficiency among selected

business organization in Nigeria, and the positive effects it has on a user's ability to render services, such as the ability to secure a network and avoid possible intrusion from hackers who may come up with a denial of service attack, viruses and spywares that tries to steal delicate and invaluable data from computer networks [18][19][20]

OBJECTIVE OF THE STUDY

The central objective of the study is to examine the effects of firewall on cost efficiency among selected business organizations in Nigeria. The specific objectives of this study are as follows:

Identify the various aspects that firewall security can be deployed within business organizations.

To examine the collective effects of all aspects of firewall system in achieving cost efficiency among business organizations.

To examine the individual effect of each aspect of firewall system in achieving cost efficiency among business organizations.

To make policy recommendations based on the findings of the study.

4. SCOPE OF THE STUDY

The scope of this work "The effects of firewall on cost efficiency among selected business organization in Nigeria'' will refer to the specific areas where a good deal of work will be done. This study analysis will concentrate on:

The Frame work of Firewall Technology systems,

The need for a firewall Security system in the field of computer networks

The Cost efficient role of using a firewall systems

The impact of firewall Technology on network security

The individual and combined effect of using firewall security system.

5. LIMITATIONS OF THE STUDY

This study will be restricted to a survey of staff of business organizations that has deployed the use of firewall technology in their organization. The limitations faced in the course of carrying out this study include:

1. Limited time
2. Inadequate literature and materials
3. Reluctance on the part of staff and customers to speak their minds freely

4. Lack of adequate funds

There was limited time frame for the analytical approach that led to these findings; the short time frame really affected the analysis of data and its collection. This work was carried out alongside with a complete academic schedule of lectures and so there was little opportunity to meet persons and people in huge and multinational establishment and study their firewall security systems at a great depth. In my own opinion I strongly believe that this study would have being so fabulous and extremely outstanding, if I do have a more balanced knowledge of other areas of computer network security. This work was also challenged with inadequacy of funds as a barrier to more exploration of data, and also reluctance and fear of meeting a stranger on the part of some staff and customers of some business organization.

6. SIGNIFICANCE OF THE STUDY

The findings of this work should be considered very worthy and experimentally implemented. There have been many losses in the field of business organization activities. More or less people have a good knowledge of what a firewall security system entails. Lesser number of people, who have the knowledge of firewalls, often carries out a poor implementation of this security system. There has been much threats posed to computer networks by unauthorized intruders who willfully gain entrance into a network by bypassing any form of security put in place by the network administrators and managers. These intruders by this very act send in a lot of risks and threats to computers and networks by sniffing out invaluable data from the network such as Username's, passwords, stealing and deletion of information stored up in several database locations, launching of DOS (Denial of service attacks) and having a mass spread of virus threats which eventually brings down the whole system. This piece of work has a great significance to the computer sector as it tries to state a refined view of the cost efficient effects of firewall security when compared to the losses associated with unprotected computer systems. Network administrators, managers and users of computer systems can equally understand the financial and operational gains attributed to firewalls when placed as a security barrier to prevent intrusion by hackers and other unwanted parties. Keeping unauthorized users such as hackers, crackers, vandals and spies out of the protected network sanitize a network, cuts down costs of running a network and counter the vulnerability of different networks.

7. RESEARCH QUESTIONS

Based on the statement of problem, the objectives of the study, the researcher pose the following questions:

To what extent do the collective aspects of firewalls affect cost efficiency among business organizations in Nigeria?

To what extent does individual aspect of firewalls affect cost efficiency among business organizations in Nigeria?

8. RESEARCH HYPOTHESIS

On the basis of the statement of problem, objectives of the study and research question, the following hypothesis have been formulated.

Ho_1: the collective aspects of firewall systems have no significant effect on cost efficiency among business organizations in Nigeria.

Ho_2: the individual aspects of firewall systems have no significant effect on cost efficiency among business organization in Nigeria.

9. RESEARCH METHODOLOGY

This research work is based on a well structured method using standard empirical tools. It also explains the knowledge of research and the technique for data gathering. The production of knowledge depends on the techniques for collecting, analyzing, and interpreting data. The research methodology consists of both qualitative and quantitative methods of data collection and empirical analysis will be employed. Again this is due to the nature of variables and context being investigated. The researcher has employed a case research approach as this method is particularly well suited for this research work. This research work refers to the use of qualitative and field based construction techniques and analysis of business cases [24]. The case study research will hence, involve data collection from sources such as questionnaires, personal interviews as the source of primary data. The research approach adopted in this research work is basically a deductive one in which the research have built hypothesis drawn from existing body of knowledge (literature review) and hence to be subjected to empirical scrutiny /testing leading to acceptance or rejection of prior hypothesis [24].

10. RESEARCH DESIGN

Kermere and Taylor (1983) emphasized that a good research design will ensure that data collected is consistent with the study of the objectives in addition to being accurate and economical. Functions of the research design include:

a. Demand for answers to questions among relationship among variables
b. Increased certainty and generalization of results

The field survey was adapted for data collection among business organization based on specific application area such as in the various departments:

Network Security; Database Security; Software Security; Hardware Security

In this study, the researcher developed a well structured standardized questionnaire based on the Likert five-point ordinal scale and they were administered to staff, experts, users, system analysts, programmers and other stakeholder in the domain of study. The respondents possess technical skills, academic qualification and a wide experience on the effects of firewalls on cost efficiency. Regarding this a total of 105 copies of questionnaires were distributed.

11. SOURCES OF DATA

The sources of data for this research work were exclusive primary data sources. Primary data sources for this research were obtained from structured and standardized copies of questionnaire targeted to 105 respondents. The respondents are professionals or stakeholders in the area of the research interest. Primary data gives credibility to the research result and as well secondary data. The secondary data included in this work includes sources from textbooks, workshop papers and journals.

12. METHOD OF DATA COLLECTION

This section deals with means and techniques through which data was collected for this research work. The primary data (copies of questionnaire) collected here were meant for testing and validating the prior hypothesis postulated through literature review which is the secondary data. In the field of computers today, business organizations deploy the use of computer systems which are also properly secured from internal and external source of risks and threats in their daily activities, an idea of the cost efficient role of firewall technology comes into play here. The researcher visited some business organizations, as well as some Information Technology oriented – business entities like: National Institute of Information Technology (NIIT), KAROX Technologies, and other establishments of Information Communication Technology (ICT).

12.1. Method of Primary data collection

The primary data collection tools are used for this research work questionnaires are administered with the Likert five-point scale. The Likert summated involves statement related to attitude in question (Osuala, 1982). The respondents are required to indicate the degree of agreement or disagreement with each statement. A numerical score is assigned is assigned to each degree of agreement / disagreement. The scores from the statement are added up to obtain the total score for each respondent. Example

Table 1: Likert five-point scale

Source: Booz Allen Hamilton 2007

Strongly disagree	1
Disagree	2
Neutral	3
Agree	4
Strongly Agree	5

12.2 SAMPLING DESIGN AND PROCEDURE

Due to limitation in resources the researcher might find it difficult to conduct total enumeration (studying the whole population). The option is to limit the study to some of the objects selected from the population sample with a view to extending the findings of the entire population.

There are many companies involved in the use of firewall systems technology across Nigeria. These companies have professionals with the several years of experience in computer security, the firewall security system, its architecture and policies. In all the business organizations, the researcher has selected a few to represent the entire population. This decision was made due to resource constraints. About 105 questionnaires were distributed to the experts who

have knowledge in the selected areas. The approach used in this survey is the simple random sampling.

TABLE 2: Sample distribution of employees

NAMES OF ORGANIZATIONS	NUMBER OF EMPLOYEES
National Institute of Information Technology	30
KAROX Technologies	20
Other Information Communication Technology(ICT) centers	40

13. QUESTIONNAIRE DISTRIBUTION

The distribution of the copies of questionnaire was purely exclusive because the respondents are expected to be highly skilled and educated in the knowledge and use of firewall systems and possibly be able to identify their effects in a networked environment and business organizations at large. The following will guide the researcher in distributing the questionnaire:

a. The respondent must be educated, at least possess WAEC/GCE or higher qualifications in computer technology and other ICT related disciplines, and must be skilled employee of the selected company.
b. He / She must be willing to respond
c. The respondent must not be less than 18 years of age and must possess not less than two (2) years of experience in the field of computer discipline. The above requirements were satisfied

14. METHOD OF DATA ANALYSIS

14.1 Multiple Regression Analysis

Multiple Regressions is a multivariate statistical technique which helps to predict one variable from other variables, as long as there are established relationships between the variables (Nworuh, 2004). The variables being predicted is usually known as dependent variables because its values is independent on the other variables. In multiple

regressions, the model relationship between the dependent variable and independent variables is as given in the equation 1.

$Y = +\beta_1X_1 + \beta_2X_2 + \beta_3X_3 + \beta_4X_4 + E_i$ … … … … … equation 1

Y = dependent variable

Where $X_1, X_2 \ldots X_n$ = independent variable

β_0 = a constant value of Y when all values are 0.

$\beta_1 + \beta_2 + \ldots + \beta_n$ = net regression coefficients. For instance,

β_0 Measures the change in $X_1 \ldots n$ while holding other variables constant.

E_i = independent and normally distributed random error term with mean zero.

For the purpose of this study, our:

Y = Cost Efficiency, the dependent Variable; X_1= Hardware Security aspect (independent variable); X_2 = Network Security aspect (independent variable); X_3 = Database Security aspect (independent variable); X_4 = Software Security aspect (independent variable)

14.2 Test of Hypothesis ($H0_1$ and $H0_2$)

Hypothesis $H0_1$ and $H0_2$ are to be using multiple regressions, Y represents cost efficiency (dependent variable) while the independent variables ($X_1 \ldots \ldots X_4$). F- test is to be employed in t each testing the overall significance of the Model (independent variables taken together), while the T-test will be employed in testing the significances of each of the independent variables.

14.3 Test of model (ANOVA)

Very often we are interested in testing whether more than two population and means are equal. The procedure for the equality of three or more means is provided by a statistical technique known as the analysis of variance (ANOVA). This method is based on the F- distribution (or F-test) and uses real scores collected from the survey. ANOVA measures whether or not the equation 1 represents a set of regression coefficients. In multiple regression, the total deviation on each observation Y_i from the mean $(Y_i - Y)$ can be expressed as the sum of its explained and unexplained variations:

$\sum(Y- Y)^2 = (\sum Y_1^2 - (Y)^2 + \sum Y_1^2 - \sum Y^2)^2$ … … … … equation 2

SST = SSR + SSE

Where $(\sum Y_1^2 - (Y)^2$ = Explained variables

$\sum Y_1^2 - \sum Y^2 =$ Unexplained variables

SST $= (\sum Y_1^2 - (Y)^2/n$ … … … … … … … … … … … … equation 3

SSE $= \sum Y_1^2 - \sum Y^2 =$ SST – SSR… … … … … ….equation 4

Where

SST = Sum of Square Total

SSR = Sum of Square Due to Regression

SSE = Sum of Square Due to Error

The necessary sums of squares, degrees of freedom, mean squares and variance ratio for multiple regressions are summarized in the ANOVA table 3 below.

TABLE 3: ANOVA Table for Multiple Regression

Source of Variation	Sum of Squares (SS)	Degree of Freedom	Mean Square	F- Ratio
Regression	SSR	K	MSR = $\frac{SSR}{K}$	F = $\frac{MSR}{MSE}$
Error	SSE	n-K-1	MSE = $\frac{SSE}{n - K-1}$	
Total	SST	N-1		

14.4 Test of the model (Coefficient of Determination and F-test approach)

One method to test statistical of estimated model is through the coefficient of determination (R^2), calculated from the Regression. R^2 gives the proportion of the total variation in the dependent variable (cost efficiency). The value R^2 ranges from 0 to 1. In setting up the test, the following Hypothesis is tested:

H_{01}: $B_1 = B_2 = 0$ (i.e. the collective aspects of firewall systems have no significant effect on cost efficiency among business organizations in Nigeria).

H_{02}: $B_1 = B_2 = 0$ (i.e. the individual aspect of firewall systems have no significant effect on cost efficiency among business organization in Nigeria).

Decision Rule

The researcher should reject H_0 if the probability of obtaining a value of the test statistics of a given or more extreme magnitude, when H_0 is true. It is equal or less than some small number. The common practice among researchers is to set the level of significance at 0.05 0r 0.01. If F-Ratio (calculated) is greater than F-ratio (tabulated), at alpha level of significance, and (K-1), (N-K) degrees of freedom, then we reject H_0 and accept H_A and then conclude that there is some truth in the estimated model (i.e. the regression model is significant since the independent variables significantly accounts for the variation in the dependent variables. Test for specific strength of independent variables: Test-Ratio.

Having established the significances of the estimated model, we now proceed to test the specific strengths of the various independent variables. This we can achieve by conduction a T-test statistics.

T-Ratio = β_k /E_i (β_k) … … … … … equation 5 for k=1 ……..8

Where

β_k = Estimate of population parameter

E_i = Standard error of the estimate

k = Number of variables

N = Number of observation

If β_k /E_i (β_k) > t_{n-k} : α /2 level of significance, we reject H_0 and accept H_A and therefore conclude that the variable belongs to the model.

15. RESEARCH FINDINGS

This section deals with the results / findings using empirical quantitative and qualitative analysis performed on the feedbacks obtained from the copies of questionnaire distributed. The data analysis techniques had to be a mixture or a variety of quantitative and qualitative methods due to the nature of phenomenon or variable(s) under study. Some variables are absolute and very easy to measure empirically while others such as service quality were more relative and hence the researcher relied on statistical tools for its analysis.

16. DATA COLLECTION AND ANALYSIS

Out of 105 copies of questionnaires distributed, 97 copies were returned. The researcher screened the copies returned for incomplete or missing data. Copies of questionnaires with mostly unanswered questions were discarded. After which we had useable survey forms, which is equivalent to 85% response rate. Statistical Package (SPSS) was used to summarize and analyze the data. Frequencies for each demographic variable(s) were computed. Reliability of the data was assessed by using Cronbach's Alpha (Cronbach, 1951; Hayes, 1998).

17. MODEL ESTIMATION AND HYPOTHESIS TESTING

The researcher conducted multiple regression analysis to examine the following hypothesis:

Ho_1: the collective aspects of firewall systems have no significant effect on cost efficiency among business organization in Nigeria.

Ho_2: the individual aspects of Firewall systems have no significant effect on cost efficiency among business organization in Nigeria.

The research seeks how well the individual and collective aspects of firewall systems affect cost efficiency among business organizations in Nigeria. Cost efficiency is an aggregation of cost reduction using hardware security aspect, software security aspect, database security aspect, network security aspect.

18. RELATIONSHIP MODEL AND ESTIMATION

In estimating the model, the summary of the data collected was subjected to multiple regression analysis using SPSS version 17. The result obtained from the multiple regression is as follows:

$R = 0.573$, $R^2 = 0.329$, adjusted $R^2 = 0.297$, $F_{cal} = 10.397$, Sig = 0.000

TABLE 4: Model Summary of the Constructs

					Change Statistics					
	R	R Square	Adjusted R Square	Std. Error of the Estimate	R Square Change	F Change	df1	df2	Sig. F Change	Durbin-Watson
1	.573[a]	.329	.297	1.25096	.329	10.397	4	85	.000	2.024

Predictors: Hardware security aspect, Software security aspect, Database security aspect, Network security aspect. Dependent Variable: Cost efficiency

Using the regression output in Table 4, we estimated the following equation: (6) the relationship model:

Overall Cost Efficiency

$= 6.604 + 0.101 X_1 + 0.130 X_2 + 0.238 X_3 + 0.183 X_4$ equation 6

X_1 = Hardware security aspect; X_2 = Software security aspect; X_3 = Database security aspect; X_4 = Network security aspect

The interpretation of the relationship model based on the output of our regression analysis as shown above is as

follows:

In equation 6 the level of relationship existing between Cost efficiency(Y) and the four explanatory variables (X_1, X_2, X_3, X_4) is shown to be strong. The R is 0.573, which indicates that 57.3% correlation exists between Cost efficiency and the aspects of firewall systems in business organizations.

Table 4 shows that 29.7 of the cumulative variations in the four independent variables of firewall systems are applied when all possible error in estimation is considered.

The standardized error in the estimation of Cost efficiency using four variables (X_1, X_2, X_3, X_4) is 1.25096

19. TEST OF HYPOTHESES

The earlier stated hypotheses are tested using the relationship model generated based on the results of the estimated coefficients and parameters.

19.1 Hypothesis One

Ho_1: the collective aspects of firewall systems play no significant role on cost efficiency among business organization in Nigeria.

In testing the hypothesis, the F_{cal} value in table 5 is compared with the F-tabulated value.

TABLE 5: ANOVA for the Constructs

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	65.083	4	16.271	10.397	.000[a]
	Residual	133.017	85	1.565		
	Total	198.100	89			

Table 5: Predictors: Hardware security aspect, Software security aspect, Database security aspect, Network Security: Dependent Variable: Cost efficiency

The F_{cal} value of 10.397 is significant at a 0.000 level which implies that testing at 0.05 level of significance, the value is highly significant. We therefore reject the null hypothesis with a conclusion that the collective aspects of firewall systems have significant effect on cost efficiency among business organizations in Nigeria.

19.2 Hypothesis Two

Ho_2: the individual aspect of Firewall systems have no significant effect on cost efficiency among business organization in Nigeria.

In order to test this hypothesis, the significance of the coefficient of each various aspects of firewall systems is shown below in table 6.

TABLE 6: T-test for the Constructs

Model	Un-standardized Coefficients		Standardized Coefficients	T	Sig.	Collinearity Statistics	
	B	Std. Error	Beta			Tolerance	VIF
1 Cost efficiency	6.604	1.735		3.807	.000		
Hardware security aspect	.101	.066	.144	1.529	.130	.892	1.121
Software security aspect	.130	.076	.168	1.709	.091	.818	1.222
Database security aspect	.238	.073	.311	3.253	.002	.862	1.161
Network security Aspect	.183	.081	.226	2.262	.026	.788	1.268

Predictors: Hardware security aspect, Software security aspect, Database security aspect, Network security aspect. Dependent Variable: Cost efficiency

H_{02A}: Hardware security aspects of firewalls do not have significant effect on cost efficiency among business organizations in Nigeria.

The t_{cal} value of 1.529 is insignificant at 0.130 level of significance, implying that testing at 0.05 level of significance, the value is insignificant. We therefore accept the null hypothesis, with a conclusion that hardware security aspect of firewalls has no significant effect on cost efficiency among business organizations in Nigeria.

H_{02B}: Software security aspects of firewall do not have significant effect on cost efficiency among business organizations in Nigeria.

The t_{cal} value of 1.709 is insignificant at 0.091 level of significance, implying that testing at 0.05 level of significance, the value is insignificant. We therefore reject the null hypothesis with a conclusion that the Software security aspect of firewalls has made significant effect on cost efficiency among business organizations in Nigeria.

H_{02C}: Database security aspects of firewall do not have significant effect on cost efficiency among business organizations in Nigeria.

The t_{cal} value of 3.253 is significant at 0.002 level of significance, implying that testing at 0.05 level of significance, the value is significant. We therefore reject the null hypothesis, with a conclusion that database security aspect of firewalls has made significant effect on cost efficiency among business organizations in Nigeria.

H_{02D}: Network security aspects of firewalls do not have significant effect on cost efficiency among business organizations in Nigeria.

The t_{cal} value of 2.262 is significant at 0.026 level of significance, implying that testing at 0.05 level of significance, the value is significant. We therefore reject the null hypothesis and accept the alternate hypothesis, with a conclusion that network security aspect of firewalls has made significant effect on cost efficiency among business organizations in Nigeria.

20. SUMMARY OF FINDINGS AND CONCLUSION

This research explored the effects of firewall on cost efficiency among selected business organizations in Nigeria. It has so far analyzed the importance and effects of firewall systems on cost efficiency among business organization in Nigeria. It was found out that proper utilization of firewalls on the various aspects of business organizations network namely: hardware security, software security, database security and network security, as a whole is fundamental to cost efficiency among business organizations. This research has shown that there are many difficulties faced by computer oriented business organizations in their daily operating activities, and the deployment of firewall security systems will go a long way in solving this problems. From the hypothesis test, it can be seen that database security aspect and network security aspects of business organizations offered a significant increase on cost efficiency among business organizations, while hardware security aspect and software security aspect made a contribution that was so insignificant. This can be as a result of poor implementation of security in the aspects of hardware and software security amongst business organizations.

When the hardware and software security aspects in computer networks of business organizations are given a good

level of priority as the database and network security aspects, there will be more contribution to cost efficiency in business organizations. Furthermore, a good understanding and proper use of firewall systems in business organizations as shown in this research work could increase cost efficiency in situations that are seen as difficult and complex among business organizations. This project has therefore shown that it is important to deploy or install firewall systems in computer networks among business organizations, as this helps in inducing a good level of cost reduction and also offers a good level of operations performance in the formal daily activities of business organizations. Information security policies should be created alongside with firewall policies. Based on the organization's information security policies, the firewall policy should be able to dictate how firewalls should handle network traffic, likewise before a firewall policy is created, some form of risk analysis should be performed to develop a list of the types of traffic needed by the organization and categorize how they must be secured including which types of traffic can traverse a firewall under what circumstances. Firewall policy should be documented in the system security plan and maintained and updated frequently as classes of new attacks or vulnerabilities arise, or as the organization's needs regarding network applications change. The policy should also include specific guidance on how to address changes to the rule set. A wise and professional use of firewall security systems will appropriately increase cost efficiency among business organizations in a way that will promote success in business organizations. Although the cost of incurring a standard firewall system may be high to some small business organizations, the long term benefits when properly utilized will reasonably justify its cost, in the reduction of daily operations cost to business organizations.

21. RECOMMENDATIONS

Based on the findings in relation to hypothesis testing, it is advisable for business organizations to see firewall systems as a necessity in their computer network environment and then reasonably spend on firewall systems. Business organizations should be able strengthen their database and network security by implementing tough firewall security policies in their networks. However, firewall systems should be made to offer enough security to hardware and software aspects of business organizations network. When firewall security systems offer much security to these aspects of business organizations network, there will be more improvement on cost efficiency.

REFERENCES

1. Alain Mayer, Avishai Wool, and Elisha Ziskind. Fang: A firewall analysis engine. In *Proceedings of the 2000 IEEE Symposium on Security and Privacy (S&P 2000)*, pages 177–187, Los Alamitos, CA, USA, May 2000. IEEE Computer Society.

2. Alec Muffett. Wan-hacking with *AutoHack (1995)* - auditing security *behind* the firewall. In *The Fifth USENIX UNIX Security Symposium*, pages 21–34, Berkeley, CA, June 1995. USENIX Association.

3. Al-Shaer E.S and H.H. Hamed (2003). Firewall policy advisor for anomaly discovery and rule editing. *8th International Symposium on Integrated Network Management*, pages 17–30, 2003

4. Andrew Molitor (1995). An architecture for advanced packet filtering. In *Proceedings of the Fifth USENIX UNIX Security Symposium*, pages 117–126, Berkeley, CA, USA, June1995. USENIX

Association
http://www.usenix.org/publications/library/proceedings/security95/fullpapers/molit_or.ps. Accessed 2002 Feb 20
http://www.aciri.org/vern/papers/norm-usenix-sec-01.pdf Accessed 2002 Feb 20.

5. Berkeley, CA, January 1992. USENIX Association
http://www.cheswick.com/ches/papers/berferd.ps Accessed 2002 Feb 20. Berkeley, CA, November 1994. USENIX Association.

6. Bruce Schneier. *Secrets and Lies: Digital Security in a Networked World*, pages 188–193. John Wiley & Sons, New York, NY, 2000.

7. Cheswick B. An evening with Berferd in which a cracker is lured, endured, and studied. In *Winter 1992 USENIX Conference, 20-24 Jan 1992, San Francisco, CA, USA*, pages 163– 173, 36

8. Computer Emergency Response Team (CERT) (2000). CERT incident note IN-2000-02 : Exploitation of unprotected windows networking shares, April 2000. http://www.cert.org/incident_notes/IN-2000-02.html.

9. Computer Emergency Response Team (CERT) (2001). CERT incident note IN-2000-03 : 911 worm, April 2000. http://www.cert.org/incident_notes/IN-2000-03.html.

10. Computer Emergency Response Team (CERT). CERT incident note IN-2001-01
Widespread compromises via “ramen” toolkit, January 2001.
http://www.cert.org/incident_notes/IN-2001-01.html.

11. Damianou, N. Dulay, E. Lapu, and M. Sloman (2001). The ponder policy specification language.

12. In *Policies for Distributed Systems and Networks. International Workshop, POLICY 2001. Proceedings, 29-31 Jan. 2001, Bristol, UK*, Berlin, Germany, 2001. Springer-Verlag. http://www.doc.ic.ac.uk/mss/Papers/Ponder-Policy01V5.pdf Accessed 2002 Feb 20

13. Elizabeth Strother (2000). Denial of service protection: the nozzle. In *Annual Computer Security Applications Conference, 11-15 Dec. 2000, New Orleans, LA, USA*, pages 32–41, Los Alamitos, CA, USA, December 2000. IEEE Computer Society. http://www.acsac.org/2000/papers/41.pdf. Accessed 2002 Feb 20

14. Frederic Avolio. Firewalls and Internet security, the second hundred (Internet) years. *The Internet Protocol Journal*, 2(2):24–32, June 1999. http://www.cisco.com/warp/public/759/ipj_2-2/ipj_2-2_fis1.html Accessed 2002 Feb 20.

15. Frederick M. Avolio and Marcus J. Ranum. A network perimeter with secure external access.

16. Fyodor. Nmap - free security scanner for network exploration and security audits, May 2004.
http://www.insecure.org/nmap. Accessed 2004 June 8.

17. Djahandari and D. Sterne. An MBone proxy for an application gateway firewall. In *Proceedings of the 1997 Conference on Security and Privacy (S&P-97)*, pages 72–81, Los Alamitos, May 4–7 1997. IEEE Press.

18. Gary B. Stone, Bert Lundy, and Geoffrey G. Xie. Network policy languages: A survey and a new approach. *IEEE Network*, 15(1):10–21, January-February 2001. 44

19. Jeffrey C. Mogul (2002). Simple and flexible datagram access controls for Unix-based gateways. In *Proceedings of the USENIX Summer 1989 Conference*, pages 203–222, Berkeley, CA, 1989. USENIX Association. ftp://ftp.digital.com/pub/Digital/WRL/ research-reports/WRL-TR-89.4.ps.gz Accessed 2002 Feb 20.

20. Julkunen H and C.E (1998). Chow. Enhance network security with dynamic packet filter. In K. Makki, I. Chalamrac, and N. Pissinou, editors, *7th International Conference on Computer Communications and Networks, 12-15 Oct. 1998, Lafayette, LA, USA*, pages 268–275, Piscataway, NJ, USA, 1998. IEEE.

21. Kai Hwang and Muralidaran Gangadharan (2001). Micro-firewalls for dynamic network security with distributed

intrusion detection. In *IEEE International Symposium on Network Computing and Applications, NCA 2001*, pages 68–79, Los Alamitos, CA, USA, 2001. IEEE Computer Society.

22. Kenneth Ingham and Stephanie Forrest (2002). A history and survey of network firewalls. Technical Report 2002-37, University of New Mexico Computer Science Department, 2002. http://www.cs.unm.edu/colloq-bin/tech_reports.cgi?ID=TR-CS-2002-37. Accessed 29 December 2002. May be accepted for publication in the International Journal of Information Security.

23. Niall McKay (2002). China: The great firewall, December 1998. Web publication: http://www.wired.com/news/politics/0,1283,16545,00.html. Accessed 2002 Feb 20.

24. Nworuh G.E (2004). Basic Research Methodology for Researcher Trainers and Trainers in Management Sciences. Second edition. Ambix, Owerri

25. Watson D, M. Smart, G.R. Malan, and F. Jahanian (2001). Protocol scrubbing: network security through transparent flow modification. In DARPA Information Survivability Conference & Exposition II, 2001. DISCEX '01. Proceedings, volume 2, pages 108– 118, Los Alamitos, CA, USA, 2001. IEEE Computer Society.