International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3759-3772 www.ijaem.net ISSN: 2395-5252

Modeling Drivers of Cybersecurity Investment Decisions for the Sustainability of Internet Services in Nigeria

[1]Student, Ugbor Ihechiluru, ElechiOnyemachi, Iwuchukwu, Vitalis .C,

Federal University of Technology, Owerri. [2]Corresponding Author: Prof. Asiegbu, B. C. Federal University of Technology, Owerri.
Federal University of Technology,Owerri.
: Federal University of Technology,Owerri.

Submitted: 15-07-2021 Revised: 29-07-2021 Accepted: 31-07-2021

ABSTRACT: Despite the several mitigation tools used by organizations (Internet Service Providers) to maintain the cybersecurity architecture, the confidentiality, integrity and availability of information, hackers have continuously evolved more sophisticated ways of hacking these techniques. Therefore, this study derived a prediction model of drivers of cybersecurity architecture investment decisions for the sustainability of internet services in Nigeria. The methods of analysis used were content analysis, cluster analysis and multiple regression analysis. The content analysis was used to identify thirty – six factors from related literature on cybersecurity architecture investment decision drivers for the sustainability of internet service provision. These factors are analyzed into six factors such as advanced in security technology, cyber risk identification and assessment, innovative cyber security decision support system, changing nature of cybersecurity threats, efficient incident and threat analysis and strengthening cybersecurity skill and expertise. The cluster analysis was used to ascertain the similarity or dissimilarity of opinion about each group of questions or factors influencing cyber security investment decision through the use of correlation method (Pearson product moment linear correlation coefficient). The data collected on individual drivers of cybersecurity investment decision were subjected to multiple regression analysis. Two major hypotheses tested, revealed that at significance level of 5% the overall drivers are significant in contributing to sustainability of cybersecurity architecture of internet service provision. The test of the significance of individual drivers revealed that each of the drivers such as: advances in security technology, cyber risk identification and assessment, innovative cybersecurity decision support system, efficient incident and threats analysis and strengthening cybersecurity skill and expertise contribute significantly to the sustainability of cybersecurity architecture of internet service provision except the changing nature of cybersecurity threat. Hence the cybersecurity investment decision drivers for the sustainability of cybersecurity architecture of internet service provision are cyber risk identification and assessment, advances in security technology, innovative cyber security decision support system, strengthening cybersecurity skill and expertise and efficient incident and threat analysis respectively. A model was thus derived to predict cybersecurity architecture investment decision for the sustainability of internet service provision. This model is of the form $Y = -2.686 + 0.395X_1 + 2.046X_2 + 0.241X_3 + (-0.531X_4) + (-0.630X_5)$. Internet service providers in Nigeria should therefore pay maximum attention to these significant drivers of investment decision in order to achieve a significant stride in sustaining cybersecurity architecture of internet service provision in Nigeria.

Keywords: Cybersecurity, investment Decision, sustainability, security architecture, significant. Drivers, Internet service provision.

1. INTRODUCTION

According to [1] "one of the biggest issues facing organizations today is how to defend themselves from potential cyber-attacks (both internally and externally). Despite the several techniques available to organizations (Internet Service Providers) to maintain the cybersecurity architecture, hackers have continuously evolved more sophisticated ways of hacking the techniques.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3759-3772 www.ijaem.net ISSN: 2395-5252

The range and manner of these unknown attacks create the need for organizations to prioritize the manner in which they defend themselves. With this each organization needs to consider the threats that are peculiar to them and act in such a way so as to reduce the vulnerability or threats". SMEs most especially are prone to these attacks partly due to lack of sophistication in their defense mechanisms, and restrictions to adequate funding for cybersecurity, to neglect of their systems by the management [2]. Unfortunately, many organizations do not carry out the analysis due to lack of available data about cost - benefits and impact of attacks. In the course of this research, a study of selected small and medium scale Internet service providers (ISPs), revealed that the funding available for cybersecurity are heavily restricted, thereby working with a fixed budget with little or no additional funding being made available for cybersecurity purposes. This budget is perceived to be insufficient to cover all the threats and vulnerabilities that their systems may experience. Furthermore; investment in cybersecurity is a strategic decision that may increase the competitive advantage of a firm over potential rivals [3]. The impact of cybersecurity to an organization has enabled them to evolve more to cybersecurity investment decisions so as to obtain the appropriate level of these investments. Some of the areas where cybersecurity spending occurs are - software to detect viruses, firewalls, sophisticated encryption techniques, intrusion detection systems, and automated data backup, and hardware devices. Instead of organizations being satisfied with their Return on Investment (ROI), cyber adversaries are breaching their systems and preventing them from accomplishing their organizational goals. Based on an understanding of the game theory approach, while the "defenders" spend more money protecting their systems from cyber attackers, the "attackers" may spend small amount of money breaching their cybersecurity controls [1]. Decision about investment should be made based on comprehensive cost – benefit analysis and risk assessment. But due to uncertainties about threats and vulnerabilities, the probabilities of having a successful attack and the efficient mitigation measures, the investment decision becomes impossible. Given the fact that there are challenges of having an adequate levels of cybersecurity under uncertainty conditions, budget constraints, an appropriate measure must be taken by an organization to ensure an adequate cyber security and to allocate resources most efficiently Indeed, organizations face a number of security challenges with respect to investment decisions in cybersecurity, the following are the challenges: business disruption as a result of network overhead from heavy security controls and this could lead to loss of reputation, productivity and revenue. [4]. In view of the above, this paper proposed a model for drivers of cybersecurity architecture investment decisions for sustainability of Internet services in Nigeria. The objective of this paper is to model drivers of cybersecurity architecture investment decisions for the sustainability of internet services in Nigeria. Two major hypotheses were tested at significance level of 5%.

II. RELATED WORKS

[5]presented a paper that provide a cybersecurity decision support system methodology and tool that can assist support security managers in calculating an optimal investment in security control. This was carried out by performing a risk analysis of the data assets of an organization and analyzing the effectiveness of different security controls against various vulnerabilities. The formulation of Control game was based on these risk assessments in order to determine the most effective way to implement each control for an organization. Their study modeled both the cybersecurity environment of an organization and non-cooperative cybersecurity control-games between the defender and the attacker which can exploit different vulnerabilities at different network locations. The methodology from their study was implemented using the SANS Top 20 Critical Security Controls and the 2011 CWE/SANS top25 most dangerous software errors. This provides cost efficient and effective solutions against commodity attacks. It is believed that this work can be used to advise security managers on how they should spend an available cybersecurity budget for their organizations. The important factors his work highlighted are that organization should know how to generate it profile appropriately because it influences the way an organization invest in their cyber security defenses. The limitation of this paper shows that the data is generated with limited set of experts as a result the cyber environment needs is not understood; Also the methodology was not implemented in a realistic environment, hence the need of this study. This work would gear producing an effective cybersecurity decision support model that will enable an organization to understand the steps of existing attacks and select which different security control to invest in.

In a paper by [6], there is an extension of previous work done in the area of decision support tool for cybersecurity investment. The authors

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3759-3772 www.ijaem.net ISSN: 2395-5252

addressed uncertainties in risk assessment that affect cybersecurity investment. The conducted an experiment on optimal cybersecurity investments under uncertainty and highlighted that even if there are uncertainty that impact payoff and viable strategies, there is still consistency where losses were mitigated with few security control. The limitation of this work is that the proposed decision support system was not applied in a realistic environment.

[7] proposed methodologies for evaluating information security investment. In his work some models were believed to be created around security investment, but the financial analysis method was not integrated. The author stated that the best known approach used in risk management and regulatory capital calculation is Loss Distribution Approach. He concluded that an appropriate method used for measuring the performance of information security investment is the risk mitigation.

[8]proposed and developed an analytical real options framework. This analytical real options framework incorporates major components relevant to cybersecurity practice. The authors analyzed how a private firm can perform an optimal cybersecurity investment decisions. Through the use of real options theory, this paper provides an analytical solution that tends to intuitive interpretations regarding the effect of timing and cybersecurity risk on investment behavior. The results from their study indicate that the value of an option to invest in cybersecurity is raised by the greater uncertainty over the cost of cybersecurity attacks. This increases the incentives to temporarily suspend operations in order to install a cybersecurity patch which will make an organization more resilient to cybersecurity breaches. Similarly, the value of the option to invest in cybersecurity is increase by the likelihood associated with the availability of a cybersecurity patch.

[9]highlighted key tasks for organization when investing in cybersecurity. Such task were: The optimal amount to invest, the technical, managerial and organizational security countermeasure that would be generated for adequate protection and how much would be spend on countermeasure due to budget constraints were decided. He also presented some techniques that could be employ in the identification of assets, threats; vulnerabilities and controls in an organizations, such techniques were as follows: Identification of organizational assets which can be applied using known information, the identification of threats or archival records of attacks in log files or threat modeling techniques such as attack graphs, attack trees or onion skin models and Vulnerabilities which can be identified using automated vulnerability scanning tools or penetration tests through the aid of databases such as the National Vulnerability Database (NVD).

In addition, [10] agreed that cyber insurance would improve the overall level of cybersecurity which would lead to higher investment decision in cybersecurity. They said that cyber-insurance standards would facilitate best practices for organization. They also outlined some of the benefits of cyber-insurance such as improving an overall societal well-being through growing insurance market in the area of cybersecurity. They conducted field study in order to understand the information security investment decision. It was discovered that the main driver that affects the existing level of the organizational information or cybersecurity was the need to protect its internal network and data. A major limitation of these papers is that cybersecurity budgets are limited but they assume that sufficient resources are available to make these investments. Some other limitations includes: The effective resource allocation is difficult due to the multiple part of uncertainty about the changing nature and incident threats and vulnerabilities evolving in an organization as well as adequate mitigating measures needed to combats the cyber attacks. The increase in attack methods/vectors were not taken into recognition. Cybersecurity skills on the part of the users are not adequate. Some organization's decision support system or tools are not adequate for decision making. This suggests the significance of this research.

III. RESEARCH HYPOTHESIS

The following hypothesis was tested using 0.05 significance level;

H_{01}: Each driver in the proposed model has no significant effect on cybersecurity architecture of Internet Services.

H_{02}: The overall drivers in the proposed model have no significant effect on cybersecurity architecture investment decisions in sustainability of Internet Service.

IV. METHODOLOGY

The researcher chose a quantitative research approach and an analytical field survey, aimed at studying relevant and related literatures to determine weaknesses with the existing investment decision variables of cybersecurity, and proposing a new model that would sustain ISPS to overcome the existing weaknesses. This model was

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3759-3772 www.ijaem.net ISSN: 2395-5252

formulated after conducting content analysis, cluster analysis and multiple regression analysis on the collected data.

i. Case Study.

The population studied in this research work comprises of 10 selected active and functional Internet Service Providers (ISPs) located in Owerri Municipal area and Port Harcourt city. As earlier stated, a total of ten (10) active ISPs were selected, with an uneven distribution of staff. In the composition of the total population, the researcher considered all the staff in these 10 ISPs, and selected experts in the field of study (decision makers); this makes our target population group finite. The simplified formula for the determination of sample size to be selected from the population of active ISPs, given by Yamane (1967) as defined in equation 1.

$$n = N/1+Ne^2 \qquad (1)$$

was used to find the sample size to be selected for the study; where n is the sample size to be selected for study, N is the population of active ISPs and e is the level of precision which will be taken as 5% (95% confidence) level. Equation (1) also referred as the YamannYaroformular for finite population was applied to reduce the large population into a smaller and manageable sample size. Then, the stratified random sampling (STRS), with proportional allocation of sample, were also adopted in the study for selecting appropriate sample of respondents or staff from each active ISPs to be studied in the study. The stratified random sample statistic is defined in equation 2.

$$n_h = \frac{N_h}{\sum_{h=1}^{N} N_h}.n \qquad (2)$$

where N_k is the staff population in the hth active ISPs organization, $\sum_{h=1}^{N} N_h$ is the overall staff population in the active ISPs organization (representing the total population), n_k is the sample size of respondents or staff selected from each hth active ISPs organization and n is the sample size determined for study using (1).The population size of one hundred and ninety-five (195) active ISPs, which reflects the number of staff (decision makers) working in the 10 identified ISPs in Owerri and Port Harcourt Municipals, were observed for the study. Hence, we select a sample of size n at 95% confidence level (α equals 5% significance limit) and were reduced a target size which was used in this research work. The sample size obtained serves as the total sample of staff selected from the active ISPs organization and this number corresponds with the number of questionnaires produced and distributed to these targeted audience.

Example 1

The Yamane Yaro formula for finite population whose statistic is given in equation 1 was applied to obtain the sample of size n at 5% significance level as

$$n = \frac{195}{1+(195*0.05^{2})} = 131$$

Therefore, a sample size of 131 respondents was used in this study. This means that a total number of 131 respondents were contacted in carrying out his study. Then, the stratified random sampling, with proportional allocation of sample whose statistic is described in (2) were used to determine the appropriate sample of respondents or staff from each active ISPs to be studied in the study

ii. Method of Data Collection

Both primary and secondary data were used in this study. The secondary data was gotten from various journals, books and other relevant related literature. The primary data was generated from administering a well-structure questionnaire to the experts in the field such as decision makers on the research subject. The researcher adopted a multiple choice, fixed format kind of questionnaire. The questionnaire is based on Likert five-point ordinal scale (1 – 5) ranging from ("Strongly Agree to Strongly Disagree") as shown in Table1. The researcher visited the ISPs in Owerri individually and distributed the questionnaire by hand to staff; while the ISPs in Port Harcourt have theirs sent to them through an electronic mail. The filled questionnaires were also returned by hand delivery, and through email respectively.

iii. Methods of Data Analysis

The use of Multiple Regression Technique and other statistical techniques for data evaluation were adopted in this research. The statistical techniques involve are:

i. Content Analysis
iii. Cluster Analysis for selection of Study Variables
iv. Detection of Multicollinearity
v. Multiple Regression Technique
vi. Residual Analysis

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3759-3772 www.ijaem.net ISSN: 2395-5252

a. Content Analysis

Different factors influencing the cybersecurity architecture for investment decisions for the sustainability of internet service provision that contributed to the same meaning were grouped into one category. This process was repeated until distinct sets of categories were obtained. Each category represents factors influencing cybersecurity architecture investment decision for the sustainability of internet service provision. This can be seen in table 2. These variables are Advances in security technology, Cyber risk identification and assessment, Innovative cybersecurity decision support system model, Changing nature of cybersecurity Threats, Strengthening cybersecurity skill and expertise and Efficient incident and threats analysis. Content Analysis was used because different items were used by different authors to identify the same factors and it is difficult to know which category a given factor belongs to. Also some factors described in those publications by these authors are not clear and require careful reading, understanding and interpretation to produce accurate findings.

Table 1: Likert five grade point scale [11]

View	Grade Points
Strongly disagree	1
Disagree	2
Neutral	3
Agree	4
Strongly Agree	5

Table 2 shows clustering of identified factors influencing cybersecurity architecture investment decision.

S/N	Factors influencing cybersecurity architecture investment decisions	Non-adopting Factors
1	Budget constraint Fears of reputation damage Rules and regulation Response to investigative capacity Management awareness/support Client requirement Supplier demand NIST/ISO publication and vendor recommendation Brand reputation	Innovative Cybersecurity Decision support model
2	Identifying the attacker's motive Vulnerabilities Probabilities of successful attack	Efficient incident and threat analysis

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3759-3772 www.ijaem.net ISSN: 2395-5252

	Breach or incident Media attention	
3	The latest technology Response to internal security compromise.	Advances in security Technology
4	Availabilities of Resources Need to protect its internal network Expectation of future threats	Changing nature of cyber security threats
5	The context establishment Risk identification Risk analysis Risk evaluation Risk treatment Business Process External audit Internal audit.	Cyber risk identification and risk assessment.
6	IT staff's knowledge and expertise Response to internal security compromise The right team with the right knowledge	Strengthening cybersecurity skill and expertise.

b. Detection of Multicolinearity

The presence of multicolinearity among the independent variables was investigated using variance inflation factor and the tolerance factors test statistics defined according to equations 3 and 4.

$$VIF = \frac{1}{1 - R_j^2} \qquad (3)$$

while the tolerance factor is

$$TF = \frac{1}{VIF} \qquad (4)$$

where R_j^2 is the multiple correlation of the independent variable, X_j as dependent variable with the other members of the independent variables, VIF is the variance inflation factor statistic and TF is the tolerance factor. Then, the decision will be to reject that there is multicolinearity among the independent variables if the value of the variance inflation factor test statistic is less than the threshold number equals ten and the value of TF is not close to zero .

c. **Multiple Regression Analysis**

Multiple Regression Analysis as a statistical technique is used in the study for estimating the relationships among or between a dependent variable and one or more independent variables (or predictors). The technique of partitioning the total variation of data into useful components is known as Analysis of variance. The means by which different sources of variation are measured is provided by the analysis of variance. In multiple regressions, the F-test statistic (F=MSR/MSE) is used in testing the equality of group (respondent) means which under the null hypothesis Ho has F (K, n-k-1) F-distribution critical value based on the chosen level with k degrees of freedom DFR and DFE. The null hypothesis states that Ho1 = HA2 = ... = Hk= 0, Ho is accepted at the significant level if F < Fi – α (k, n-k-1) otherwise, Ho is rejected in favour of HA: F1-α (k, n-k-1) from the statistical table. $\gamma = \beta_o + \beta_1 X_1 + \beta_2 X_2 + \cdots + \beta n X n + \epsilon_1$

γ=Dependent variable
$X_1, X_2, \ldots, Xn$ are the independent variables
β_o=a constant value of γ when all X values are 0

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3759-3772 www.ijaem.net ISSN: 2395-5252

ϵ_1=independent and normally distributed random error term
For the purpose of this study:
γ=Investment Decisions for Sustainable Internet Service Provision
X_1=Advances in Security Technology
X_2=Cyber risk Identification and Assessment
X_3= Innovative Cybersecurity Decision Support Model
X_4=Changing Nature of Cybersecurity Threats
X_5= Strengthening Cybersecurity skill and Expertise
X_6 = Efficient Incidents and Threat Analysis

d. **Decision Rule**

In testing the null hypothesis stated in this study, the following rule was adhered to in deciding whether to accept or reject the null hypothesis: Reject the null hypothesis (Ho) if the calculated probability value is less than the significant level of 0.05, else accept null hypothesis. When the null hypothesis is rejected, the alternative hypothesis (Ha) is accepted and vice versa.

V. MULTIPLE REGRESSION PARAMETER ESTIMATION AND MODEL FORMULATION

The structural representation of the proposed multiple regression model, to establish a linear relationship between **t**he overall drivers in the proposed for study and cybersecurity architecture investment decisions in sustainability of services of internet providers is:

$$Y_i=\beta_0+\beta_1 X_{1i}+\beta_2 X_{2i}+\beta_3 X_{3i}+\beta_4 X_{4i}+\beta_5 X_{5i}+e_i \;\nabla i=1,2,...,n \quad (5)$$

where $\hat{\beta}_0, \hat{\beta}_1, \hat{\beta}_2, ..., \hat{\beta}_5$ are the estimated intercept and the regression coefficients of the multiple regression model, $Y, X_1, X_2, ..., X_5$ retain their defined meanings, n is the number of respondents or staff whose opinions were surveyed, $\mathbf{X}$ is the $n\times(k+1)$ matrix of observations or model specification matrix of the independent variables, $\mathbf{Y}$ is the $(n\times 1)$ vector of the dependent variables, $\hat{\boldsymbol{\beta}}$ is the $(k+1)\times 1$ vector of the estimated model parameters and k is the number of estimated regression coefficients which is equal to six. The total variation which is partitioned into its recognizable sources of variation is presented using Analysis of Variance (ANOVA) shown in Table 3. The ANOVA Table was employed in the study to ascertain the significant of the regression coefficient of both the existing drivers of cybersecurity architecture investment drivers in the literature and the overall drivers proposed for study in sustainability of service of internet providers; in order to ascertain hypotheses H_{01} *and* H_{03}. $\hat{\sigma}^2$ is the estimated error variance, SSE is the error sum of squares, DF_{error} is the degree of freedom due to error, SST is the sum of squares due to total variation, SSR is the regression sum of square, $\bar{Y}$ is the mean of Y_i and $\hat{Y}_i$ is the estimated fit of Y_i which is explained by the regression model.

VI. RESULTS

i. Test For Significance Of Regression For Each Driver Of Cybersecurity Architecture Investment Decisions

The significance of regression for each driver of cybersecurity architecture investment decisions X (Average responses on Advances in security technology (denoted X_1) Average responses on Cyber risk Identification and Assessment (denoted X_2), Average responses on Innovative cybersecurity Decision Support Model (denoted X_3), Average responses on Changing nature of cybersecurity Threats (denoted X_4), Average responses on Strengthening cybersecurity Expertise (denoted X_5) and Average responses on Efficient incidents and threat analysis (denoted X_6)) in explaining the sustainability of internet service provision in Nigeria was ascertained in the study using the student t distribution test defined in equation 6. (Walpole et al, 2007)

$$t=\frac{b_j-\beta_{j0}}{\hat{\sigma}\sqrt{c_{jj}}};\; j=1,2,...,6 \quad (6)$$

where b_j is the jth estimated regression coefficient of Y on X, $\hat{\sigma}\sqrt{c_{jj}}$ is the standard error of each jth estimated regression coefficient of Y on X and β_{j0} is the jth null value of the regression coefficient of Y on X, will be employed to test the significant effect of each driver of cybersecurity architecture investment decisions in sustainability of internet service provision in Nigeria. The test statistic in Equation (6), under the null hypothesis

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3759-3772 www.ijaem.net ISSN: 2395-5252

$(H_0 : \beta = \beta_{j0} = 0)$ of no significance effect of each driver of cybersecurityarchitecture investment decisions X on Y follows the student t distribution. Then, the decision rule will be to reject the null hypothesis at level α if the value of t is larger than the $1-\alpha/2$ quartile of the student t distribution with $n-2$ degree of freedom and n is the number of observations or respondents.

ii. Test For Significant Regression Of The Overall Drivers Of Cybersecurity

By adopting the Analysis of Variance Technique in Table 3, the significance of the overall drivers proposed in the study for sustainability of service of internet providers was tested using the F distribution test. The test statistic is defined in equation 7

$$F = \frac{MSR}{MSE} = \frac{SSR/k}{SSE/(n-k-1)} \quad (7)$$

under the null hypothesis

$(H_0 : \beta_1 = \beta_2 = ... = \beta_k = 0$ for the proposed model) of no significance effect of $\mathbf{X}$ on $\mathbf{Y}$ follows the F distribution with $(m, n-k-1)$ degrees of freedom; where n is the number of observations or respondents, MSR is the mean sum of squares due to regression, MSE is the mean sum of square due to error, k is the degree of freedom due to regression and $(n-k-1)$ is the degree of freedom due to error. Then, the decision rule will be to reject the null hypothesis at level α if the value of F is larger than the 1-λ quartile of the F distribution and conclude that there is significant different of the overall drivers proposed for study in sustainability of service of internet providers.

iii. Test Testof the Predictability Strength of Independent Variables in the Model

The values of the multiple regression model summary statistics (multiple correlation coefficient (R), coefficient of determination (R^2 or R Square) etc are shown in Table 4. The result in Table 4 shows that the value of the multiple correlation coefficients (R) is 0.902 or 90.2% which indicates a strong positive relationship between the dependent and independent variables. **S**imilarly, the value of the coefficient of determination (R^2 or R Square) of the multiple regression model is 0.814 or 81.4% which indicates that about 81.4% in the variation of responses on cybersecurity for the sustainability of internet service provisions can be explained and/or predicted by the independent variables (Average responses on Advances in security technology (denoted X_1), Average responses on Cyber risk identification and assessment (denoted X_2), Average responses on Innovative cybersecurity decision support model (denoted X_3), Average responses on Changing nature of cybersecurity Threats (denoted X_4) and Average responses on Strengthening cyber security skill and expertise (denoted X_5) and Average responses on Efficient incidents and threat Analysis (denoted X_6)). The value of the coefficient of determination (R^2 or R Square) of the multiple regression models equals 0.814 or 81.4% also show that about 0.186 or 18.6% of the total variation is attributed to the error associated with the model while 81.4% of the total variation is accounted by the model. The result also supports the assertion that the independent variables are good predictor of the dependent variable. The result also supported the finding that there is significant correlation between the dependent and independent variables because any change in the predictor variables accounts for a significant change of about 81.4%% variation in the dependent variable. Furthermore, the value of the Durbin Watson test statistic equals 2.053 is greater than the tabulated lower critical value, for the 131 observations of the six predictor variables, equals 1.70. This result confirmed that the residual from the resulting model are uncorrelated and as a result the assumption (structureless and uncorrelation of residuals) of the multiple regression model is not violated.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3759-3772 www.ijaem.net ISSN: 2395-5252

TABLE 4: VALUES OF THE MULTIPLE REGRESSION MODEL SUMMARY STATISTICS

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics					Durbin-Watson
					R Square Change	F Change	df1	df2	Sig. F Change	
1	.902[a]	.814	.805	.16578	.814	90.478	6	124	.000	2.053

*

Similarly, the value of the coefficient of determination (R^2 or R Square) of the multiple regression model is 0.814 or 81.4% which indicates that about 81.4% in the variation of responses on cybersecurity for the sustainability of internet service provisions can be explained and/or predicted by the independent variables (Average responses on Advances in security technology (denoted X_1), Average responses on Cyber risk identification and assessment (denoted X_2), Average responses on Innovative cybersecurity decision support model (denoted X_3), Average responses on Changing nature of cybersecurity threats (denoted X_4) and Average responses on Strengthening cybersecurity skill and expertise (denoted X_5) and Average responses on Efficient incidents and threat analysis (denoted X_6)). The value of the coefficient of determination (R^2 or R Square) of the multiple regression models equals 0.814 or 81.4% also show that about 0.186 or 18.6% of the total variation is attributed to the error associated with the model while 81.4% of the total variation is accounted by the model. The result also supports the assertion that the independent variables are good predictor of the dependent variable. The result also supported the finding that there is significant correlation between the dependent and independent variables because any change in the predictor variables accounts for a significant change of about 81.4%% variation in the dependent variable. Furthermore, the value of the Durbin Watson test statistic equals 2.053 is greater than the tabulated upper critical value, for the 131 observations of the six predictor variables, equals 1.81. This result confirmed that the residual from the resulting multiple regression model fitted to the study data are uncorrelated and as a result the assumption (structureless and uncorrelation of residuals) of the multiple regression model is not violated.

iv. Model Estimation and ANOVAs for the Constructs

The estimates of the coefficient of the impact of the independent variables (Predictors variables: Average responses on Advances in security technology (denoted X_1), Average responses on Cyber risk Identification and Assessment (denoted X_2), Average responses on Innovative cybersecurity decision support model (denoted X_3), Average responses on Changing nature of cybersecurity Threats (denoted X_4), Average responses on Strengthening cybersecurity skill and expertise (denoted X_5)and Average responses on Efficient incidents and threat analysis. (denoted X_6)) in sustainability of internet service provisions are shown in Table 5. The value of the constant term is -2.686 while the values of the regression coefficients of the proposed multiple regression models lie between -0.630 to 2.046. The p values lie between 0.000 and 0.202. Similarly, the t value of the constant term is -6.536 and the absolute t values for the regression coefficients lie between 1.283 and 9.859. The result indicates that the p values of the constant term and that for some regression coefficients

$(\hat{\beta}_1 equals 0.395, \hat{\beta}_2 equals 2.046, \hat{\beta}_3 equals 0.241, \hat{\beta}_5 equals -0.531 \text{ and } \hat{\beta}_6 equals -0.630)$

are less than 0.05 level of significance while the absolute value of the t values of the corresponding regression coefficients are greater than the 0.975 quartile of the tabulated student t distribution at 125 degree of freedom equals 1.96. The result also indicates that the p value of the regression coefficients $(\hat{\beta}_4 equals 0.102)$ is greater than 0.05 level of significance while the absolute value of the t value (1.283) of the corresponding regression coefficient is less than the 0.975 quartile of the tabulated student t distribution at 125 degree of freedom equals 1.96.These results indicated that the constant term and the regression coefficients

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3759-3772 www.ijaem.net ISSN: 2395-5252

$(\hat{\beta}_1 equals 0.395, \hat{\beta}_2 equals 2.046, \hat{\beta}_3 equals 0.241, \hat{\beta}_4 equals -0.531 \text{ and } \hat{\beta}_5 equals -0.630)$

contributes significantly to the ability of the proposed multiple regression model in explaining the sustainability of internet service provisions in Nigeria while the regression coefficients $(\hat{\beta}_4 equals 0.102)$ is not significant . However, the proposed multiple regression models considered in the work is

$\hat{Y}_i = \hat{\beta}_0 + \hat{\beta}_1 X_{1i} + \hat{\beta}_2 X_{2i} + \hat{\beta}_3 X_{3i} + \hat{\beta}_4 X_{4i} + \hat{\beta}_5 X_{5i} + \hat{\beta}_6 X_{6i} + e_i \ \nabla i = 1,2,..$
(Milton and Arnold, 1995)

Where from Table 5, therefore, the estimated (fitted) regression model is

$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \beta_5 X_5 + \beta_6 X_6 + €$ (11)

$\hat{\beta}_0 equals -2.66,$

$\beta_1 equals 0.395, \ \beta_2 equals 2.046, \beta_3 equals 0.241, \beta_4 equals 0.102, \ \beta_5 equals -0.531 \text{ and } \beta_6 equals -0.630.$

$Y = -2.66 + (0.395X_1) + (2.046X_2) + (0.241X_3) + (0.102X_4) - (0.531X_5) - (0.630X_6).$

Similarly, the ANOVA for the constructs are shown in Table 6. From Table 6, the combination of the independent variables in the proposed estimated multiple regression models yielded F ratio of 90.478 with a p value of 0.000. The value of F ratio equals 90.478 is greater than the tabulated value of the 0.975 quartile of F distribution at (6, 124) degrees of freedom which is equal to 2.76 while the p value of 0.000 is less than the 0.05 level of significance. This result shows that the collective cyber security investment factors; Average responses on Advances in security technology (denoted X_1), Average responses on Cyber risk identification and assessment (denoted X_2), Average responses on Innovative cybersecurity decision support model (denoted X_3), Average responses on Changing nature of cybersecurity threats (denoted X_4), Average responses on Strengthening cybersecurity skill and expertise (denoted X_5) and Average responses on Efficient incidents and threat analysis (denoted X_6); have significant effect on Average responses for the sustainability of service of internet providers.

TABLE 5: COEFFICIENT OF THE IMPACT OF THE INDEPENDENT VARIABLES ON THE DEPENDENT VARIABLE

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	-2.686	.411		-6.536	.000		
	X1	.395	.050	.418	7.984	.000	.546	1.832
	X2	2.046	.208	1.003	9.859	.000	.145	6.906
	X3	.241	.074	.208	3.277	.001	.373	2.683
	X4	.102	.080	.068	1.283	.202	.531	1.884
	X5	-.531	.100	-.310	-5.334	.000	.443	2.256
	X6	-.630	.104	-.498	-6.047	.000	.221	4.529

(IBM SPSS, Version Statistics 20)

v. **Test for the Relative Contribution of the individual Independent Variables**

From Table 5, the Beta values of the unstandardized coefficients, which is the proposed multiple regression coefficients employed for the derivation of the parameters of the model, obtained are 0.395, 2.046, 0.241, 0.102, -0.531 and -0.630 for the effects of Average responses on Advances in security technology (denoted X_1), Average responses on Cyber risk

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3759-3772 www.ijaem.net ISSN: 2395-5252

TABLE 6: ANOVA FOR CONSTRUCTS

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	14.919	6	2.487	90.478	.000[b]
	Residual	3.408	124	.027		
	Total	18.327	130			

1. That cyber risk identification and assessment factor made the highest significant effect followed by advance in security technology, innovative cybersecurity decision support system model, efficient incident and threat analysis and changing nature of cybersecurity threats which also contributed moderately while strengthening cybersecurity skill and expertise has the lowest effects in sustaining the services of internet provision in Nigeria.

identification and assessment (denoted X_2), Average responses on Innovative cybersecurity decision support system model (denoted X_3), Average responses on Changing nature of cybersecurity Threats (denoted X_4), Average responses on Strengthening cybersecurity skill and expertise (denoted X_5) and Average responses on Efficient incidents and threat analysis (denoted X_6) on the sustainability of service of internet providers while, that for the associated Beta values of the standardized coefficients, which have been converted to the same measurement scale for easy comparisons of coefficients values; obtained are 0.418, 1.003, 0.208, 0.068, -0.310 and -0.498. The result shows that Average responses on Cyber risk identification and assessment (denoted X_2) with the highest coefficient value of 1.003 (100.3%) exerted the greatest positive effect in explaining the variability of the sustainability of service of internet providers followed by Average responses on Advances in security technology (denoted X_1), Average responses on Innovative cybersecurity decision support system model (denoted X_3), Average responses on Changing nature of cybersecurity Threats (denoted X_4), Average responses on Strengthening cybersecurity skill and expertise (denoted X_5) and Average responses on Efficient Incidents and Threat Analysis (denoted X_6). The result also indicates that links embedded in Average responses on Cyber risk Identification and Assessment (denoted X_2) with $(\hat{\beta}_2 = 2.046, t = 9.859, P = 0.00 < 0.05)$ makes the highest significant contribution to explanation of the variability of the sustainability of service of internet provision in the proposed model followed by Average responses on Advanced in security technology (denoted X_1) with $(\hat{\beta}_1 = 0.395, t = 7.984, P = 0.00 < 0.05$),Average responses on Innovative cybersecurity decision support system model (denoted X_3) with $(\hat{\beta}_3 = 0.241, t = 3.277, P = 0.001 < 0.05)$, Average responses on Strengthening cybersecurity skill and Expertise (denoted X_5) with $(\hat{\beta}_5 = -0.531, t = -5.334, P = 0.00 < 0.05)$ and Average responses on Efficient incident and threat analysis (denoted X_6)with $(\hat{\beta}_6 = -0.630, t = -6.047, P = 0.00 < 0.05)$ while there is no significant contribution of Average responses on Changing nature of cybersecurity threats (denoted X_4) with $(\hat{\beta}_4 = 0.102, t = 1.283, P = 0.202 > 0.05)$.

These results generally showed that the drivers (X_2, X_1, X3, X5, X_6,) in the proposed model significantly affected the cyber security architecture investment decisions in sustainability of service of internet provision in Nigeria except that on Changing nature of cybersecurity threats (X_4).

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3759-3772 www.ijaem.net ISSN: 2395-5252

VII. TEST OF HYPOTHESES

This Section shows the result of hypotheses tests proposed in the study. ($\mathbf{H_{01}}$: Each driver in the proposed model has no significant effect on cybersecurity architecture investment decisions in sustainability of service of internet provision). ($\mathbf{H_{02}}$: The overall drivers in the overall proposed model have no significant effect on cybersecurity architecture investment decisions in sustainability of service of internet provision).

Results for Hypothesis One

Test of hypothesis one

1 $\mathbf{H_{01}}$: Each driver in the proposed model has no significant effect on cyber security architecture investment decisions in sustainability of service of internet provision.

$\mathbf{H_{O1a}}$: Advanced in security technology has no significant effect on cybersecurity architecture investment decisions in sustainability of service of internet provision.

$\mathbf{H_{O1b}}$: Cyber risk identification and assessment has no significant effect on cybersecurity architecture investment decisions in sustainability service of internet provision.

$\mathbf{H_{O1c}}$: Innovation cybersecurity decision support system has no significant effect on cybersecurity architecture investment decisions in sustainability service of internet provision.

$\mathbf{H_{O1d}}$: Changing nature of cybersecurity Threats has no significant effect on cybersecurity architecture investment decisions in sustainability of service of internet provision.

$\mathbf{H_{O1e}}$: Strengthening cybersecurity skill and expertise has no significant effect on cybersecurity architecture investment decisions in sustainability of service of internet provision.

$\mathbf{H_{O1f}}$: Efficient incidents and threat analysis has no significant effect on cybersecurity architecture investment decisions in sustainability of service of internet provision against the alternative.

$\mathbf{H_{11}}$: Each driver in the proposed model has significant effect on cybersecurity architecture investment decisions in sustainability of service of internet provision.

The content in Table 5 shows the report of the unstandardized and standardized coefficient of impact for each independent variable in explaining the variability in the sustainability of cyber security architecture of internet service provisions.

i. Test for Hypotheses for Each Driver in the Proposed Model for the Sustainability of Internet Services.

The result shows that X_1 which is the average responses on **Advances in Security Technology** as (β_1 = 0.395), (Beta = 0.418; P = 0.000; Tolerance = 0.546) as P < 0.05, is significant. Thus this combination of variable significantly predict the dependent variable (t = 7.984; P = 0.000 < 0.05). This indicates that Advances in security technology has a significant effect in the sustainability of internet service provision. Therefore HO_1 is rejected; HA_1 is accepted.

Cyber Risk Identification and Assessment denoted as X_2shows that (β_2 = 2.046; Beta = 1.003; P = 0.000; Tolerance = 0.145) as P < 0.05, is significant. Thus this combination of variable significant predict the dependent variable (t = 9.859; P = 0.000 < 0.05).This also indicates that Cyber Risk Identification has a significant effect in the sustainability of the internet service provision. Therefore HO_2 is rejected; HA_2 is accepted.

Innovative Cyber Security Decision Support System Model denoted as X_3 shows that (β_3 = 0.241; Beta = 0.208; P = 0.001; Tolerance = 0.373) as P < 0.05, is significant. Thus this combination of variable significant predict the dependent variable (t = 3.277; P = 0.001 < 0.05).This also indicates that Innovative cybersecurity decision support system significant effect in the sustainability of the internet service provision. Therefore HO_3 is rejected; HA_3 is accepted.

Changing Nature of Cyber Security Threat denoted as X_4shows that as (β_4 = 0.102; Beta = 0.068; P = 0.202; Tolerance = 0.531) as P > 0.05, is not significant (t = 1.283; P = 0.202 > 0.05). Thus this indicates that Changing nature of cybersecurity threats has no significant effect in the sustainability of the internet service provision. Therefore HO_4 is accepted; HA_4 is rejected.

Strengthening Cyber Security Expertise denoted as X_5shows that (β_5 = -0.531; Beta = -0.310; P = 0.000; Tolerance = 0.443) as P < 0.05, is significant. Thus this combination of variable significant predict the dependent variable (t = -5.334; P = 0.000 < 0.05).This also indicates that Strengthening cybersecurity skill and expertise has a significant effect in the sustainability of the internet service provision. Therefore HO_5 is rejected; HA_5 is accepted.

Efficient Incidents and Threat Analysis denoted as X_6 shows that (β_6 = -0.630; Beta = -

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3759-3772 www.ijaem.net ISSN: 2395-5252

0.498; P = 0.000; Tolerance = 0.221) as P < 0.05, is significant. Thus this combination of variable significant predict the dependent variable (t = -6.047; P = 0.000 < 0.05).This also indicates that Efficient incidents and threat analysis has significant effect in the sustainability of the internet service provision. Therefore HO_6 is rejected; HA_6 is accepted.

ii. Results for Hypothesis Two

Research hypothesis two are

H_{02}: The overall drivers in the proposed model have no significant effect on cybersecurity architecture investment decisions in sustainability of service of internet provision against the alternative

H_{12}: The overall drivers in the proposed model have significant effect on cybersecurity architecture investment decisions in sustainability of service of internet provision

The content in Tables 6 shows the indices for ascertaining the model significance and report for the analysis of variance of the general significance of the model.. The result show that the values of the coefficient of determination (R^2) and adjusted R^2 are 0.814 respectively, the standard error of estimation is 0.1658, the p value 0.000 while the calculated F distribution ratio is 90.478. The value of the coefficient of determination (R^2) and adjusted R^2 equals 0.814 and 0.805 respectively implies that about 81% in the variability of the dependent variable has been accounted for by the proposed model. The combination of the overall drivers in the proposed model yielded the result that the calculated Fisher distribution ratio equals 90.478 is greater than the tabulated value of the 0.975 quartile of F distribution at (6, 124) degrees of freedom which is equal to 2.76 while the resulting p value equals 0.000 is less than the 0.05 level of significance. These results lead to the rejection of the null hypothesis that the overall drivers in the proposed model have no significant effect on cyber security investment decisions in sustainability of service of internet provision and the alternative hypothesis is not rejected.

iii. Summary and Result of Hypothesis Test on the Regression Coefficients

Table 7 and 8 show the summary and result of hypothesis test on the coefficients of impact for the drivers of cybersecurity architecture investment decision variables (independent variables).

TABLE 7: SUMMARY OF HYPOTHESIS TEST

Decision Variables	Unstandardized Coefficients	standardized Coefficients	Probability value
	Beta	Beta	P
X_1	0.395	0.418	P= 0.000< 0.05*
X_2	2.046	1.003	P= 0.000< 0.05*
X_3	0.241	0.208	P= 0.001< 0.05*
X_4	0.102	0.068	P= 0.202> 0.05*
X_5	-0.531	-0.310	P= 0.000 < 0.05*
X_6	-0.630	-0.498	P= 0.000 < 0.05*

VIII. CONCLUSION

Based on the result of the study, the following conclusions were drawn

2. That collectively, the overall factors such as advances in security technology, cyber risk identification and assessment, innovative cyber security decision support system model, changing nature of cybersecurity threats, efficient incident and threat analysis and strengthening cybersecurity skill and expertise have significant influence on the cybersecurity architecture investment decision in Nigeria. Also all these factors contributed significantly in sustaining the services of internet provision in Nigeria by 81.4%.

3. That individually, each of the factors contributed significantly in sustaining the service of internet provision in Nigeria except changing nature of cybersecurity threats. This is because from the analysis, changing nature of cybersecurity threats has no significant effect in the sustainability of internet service provision.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3759-3772 www.ijaem.net ISSN: 2395-5252

TABLE 8: RESULT OF HYPOTHESIS TEST

Decision Variables	Hypothesis not rejected	Results
X_1	H_{11}	Significant
X_2	H_{11}	Significant
X_3	H_{11}	Significant
X_4	H_{01}	Not Significant
X_5	H_{11}	Significant
X_6	H_{11}	Significant

REFERENCES

[1] Meland, Tondel and Solhaug. (2015): Mitigating risk with Cyberinsurance as a Risk Management Strategy: Knowledge Gaps and Recommendation for Further Research."IEEE Security & Privacy, vol.13, No.6, pp. 38 – 43, November, 2015.

[2] Pivoriene, (2017): Real options and Discounted cash flow analysis to Assess Strategic Investment Projects April 2017 Kaunas University of Technology Lithuania April 2017, 30, 91 – 101.

[3] Kort, Murto and Pawlina, (2010): Uncertainty and Stepwise Investment. European Journal of Operational Research 202; 196 – 203 Vol 32 No 1 -4.

[4] Jakoubiet. al., (2009): A Survey of Scientific Approach Considering the Integration of security and Risk Aspects into Business Process Management. 20th International workshop on Database and Expert system. 2009.

[5] Panaousis, E. Fielder, A.Malacaria, P. Hankin, C. and Smeraldi, F. (2014): "Cybersecurity games and investments: A decision support approach,"in Proc. of the 5th International Conference on Decision and Game Theory for Security. European Journal of Operational Research, vol. 202, no. 1, pp. 196–203.

[6] Andrew F. et al. (2018): Risk Assessment Uncertainties in Cybersecurity Investments 9(2) 34. https: // doi. org/10. 3390/g 9020034.

[7] Christian Locher (2005): Methodologies of Evaluating Information Security Investments ECIS 2005 proceedings. 1561 – 1573.

[8] Chronopoulos et.al. (2017): Sequential Investment in renewable energy technologies under policy uncertainty. Energy policy volume 137, 2017.

[9] Weishaupl, Eva (2017): Towards a Multi-Objective Optimization Model to Support Information Security Investment Decision Making: Proceeding of the 4th workshop on security in highly connected IT Systems June 2017. Pp 37 – 42.

[10] Kesan, Jay, RupertoMajuca& William Yurcik.(2005): Cyberinsurance as a Market-Based Solution to the Problem of Cybersecurity – A Case Study. Illinois: University of Illinois.

[11] Susan Jamieson (2017): Likert-Scale to SAGE publication Encyclopedia of Epidemiology (2017) pp.3-5