Cost-Benefit Analysis of Cyber-Security Systems

Alese Boniface Kayode, Gabriel Junior Arome, *Member, IAENG*, Ayodele Tolulope and Akinsowon Omoyele Ajoke

Abstract—**Cost benefit analysis (CBA) is a systematic process for calculating and comparing benefits and costs of a project, decision or policy with the aim of determining if a particular project or policy is a sound investment or not .In CBA, the Total Expected Cost of each option is compared against the total expected benefits, to see the one that outweighs the other. This paper aims at carrying out the Cost Benefit Analysis of Cyber Security System investments. Cost and Benefits were expressed in monetary terms, and were adjusted for the time value of money so that all flows of benefits and flows of project costs overtime are expressed on a common basis. Individuals from the academia, financial institutions and Internet Service Providers were interviewed on the effectiveness, advantages and disadvantages of the various security strategies they deploy. This information gathered, provided the basis for carrying out a proper estimation of the costs and benefits associated with cyber security systems. Mathematical models formulated were implemented; a software was developed to copy the behavior of the models such that, costs and benefits of the cyber security strategies used are estimated by the entry of the monetary values associated with those security mechanisms**.

Index Terms--**Cost-Benefit-Analysis, Cyber-Crime, Cyber-Security, Internet, Risk-Management**

I INTRODUCTION

The Internet allows users to gather, store, process, and transfer vast amounts of data, including proprietary and sensitive business, transactional, and personal data. At the same time those businesses and consumers rely more and more on such capabilities, cyber security threats continue to plague the Internet economy. Cybercrime is the criminal activities involving information Technology Infrastructure, including illegal access, Illegal Interception, Data Interference, System Interference, misuse of Devices, Forgery and Fraud [1].

Cyber-crime is one of the dominant forms of crime that is widely being perpetrated by tertiary institution students in Nigeria [1]. Indeed, the recognition of this growing acceptance of cyber-crime, otherwise known as yahoo-yahoo in Nigeria, as a way of life among the youths has compelled the federal government to formulate measures to contain the trend at different points in time. The problem has, however, remained pervasive, despite past efforts put in place to curtail it.

Cyber-security threats evolve as rapidly as the Internet expands, and the associated risks are becoming increasingly global. Staying protected against cyber-security threats requires all users, even the most sophisticated ones, to be aware of the threats and improve their security practices on an ongoing basis. Cybercrime remains elusive and as it strives to hide itself in the face of development [3]. Creating incentives to motivate all parties in the Internet economy to make appropriate security investments requires technical and public policy measures that are carefully balanced to heighten cyber-security without creating barriers to innovation, economic growth, and the free flow of information. Yet reaching this goal is not an easy task. Cyber-security has associated costs and threats such as Hacking, Cracking, Cyber-Terrorism, Cyber -Grooming, Cyber-Pornography, Cyber-Stalking, Phishing, Piracy, Malware attack, and so on.

The constantly evolving nature of threats and vulnerabilities not only affects individual firms and their customers, but collectively the threats pose a persistent economic and national security challenge. Sharing responsibility to protect cyber security across all relevant sectors is becoming ever more important. Computing devices are highly and increasingly interconnected, which means security deficiencies in a limited number of systems can be exploited to launch cyber intrusions or attacks on other systems.

CBA is well established in microeconomics and management accounting theory, and can be used to determine estimated levels of expenditures appropriate to the values of assets requiring protection. CBA is application independent, and it involves identification and measurement of all related costs and benefits. CBA techniques provide very important metrics that could be applied to the assessment of cyber-security systems.

This work will aid the comparison of cost and benefits of cyber-security both internationally and locally,

II. MOTIVATION

Many problems in cyber security are becoming complicated and global. In July 2009, one third of South Korea's websites were knocked out over a period of a week by distributed cyber-attacks. This attack was sophisticatedly designed with a series of hierarchy--a 'host computer' which sent attack commands to infected computers, 748

Manuscript received July 01, 2016. Revised July 07, 2016

B. K. Alese is with the Computer Science Department of The Federal University of Technology, P.M.B. 704, Akure, Ondo State Nigeria. Phone: +2348034540465; e-mail: bkalese@fut.edu.ng.

J. A. Gabriel is with Computer Science Department of The Federal University of Technology, P.M.B. 704, Akure, Ondo State Nigeria. Phone: +2348068991644; e-mail: ajgabriel@futa.edu.ng

T. Ayodele is with the Computer Science Department of The Federal University of Technology, P.M.B. 704, Akure, Ondo State Nigeria. Phone: +2348136266933; e-mail: ayodeltolulope@yahoo.com.

O. A. Akinsowon is with the Computer Science Department of The Federal University of Technology, P.M.B. 704, Akure, Ondo State Nigeria. Phone: +2347039111555; e-mail: maggijoke2002@yahoo.com.

intermediate 'handlers' over 72 countries, which are infected by the host and distributed the infection, and 'agents' which are a large number of zombie PCs. Along with this chain of command, a hacker could control 130,000 zombie PCs and ordered them to attack target servers in Korea. This single crisis involved computers over 75 countries and is one of the most common types of cyber-attacks, Distributed Denial of Service (DDos) [5]. The story shows that cyber-crimes are becoming complicated and globalized. We are connected and cyber security problems are border-less. To address those types of the emerging cyber problems, we need internationally cooperative solutions.

Cyber-crime is one of the vices that is slowing down the wheels of growth of developing countries. It is currently very predominant in university towns and villages. Cybercafés have become cybercrime cafés, the high sales of Modem in the market is basically for this purpose. Pornography is now a common site on IT gadgets notwithstanding gender or age. Aside the availability and the usage of Internet based tools in Cyber Cafés for scam mails and other cyber-crimes, the growth of fixed wireless facilities in the Nigeria Scenery has aided cyber-crimes.

With concentrated cost and diffuse benefit, no entity will volunteer to solve the problems associated with cyber-security systems. With the traditional cost-benefit analysis, the benefits of international activities in cyber-security have been overlooked. More players and more activities will strengthen IT infrastructure and improve cyber security, thereby creating greater shared values all over the world.

Cyber-crime could be worst due to the subtlety of its operations and most especially the perceived heavy presence of the youths (the productive age group) in cybercrime perpetration in Nigeria. The growth of fixed wireless facilities in the Nigerian network scenery has aided cybercrimes. Fraudsters who can afford to pay for the internet connection via fixed wireless lines can now perpetrate their evil acts within the comfort of their homes. In some cyber cafes, a number of systems/cables are dedicated to cyber criminals (called “yahoo boys”) while others share their bandwidth in order to perpetrate their evil from home.

This study recognizes the lack of institutionalized solutions, and aims to provide a novel framework with which to evaluate emerging solutions to cybercrime globally. This work also reveals overlooked benefits and shared value for public agents and private companies to attain through international involvement in cyber security. The extended cost-benefit framework to be presented by this project will aid the verification of the effectiveness of cyber-security investment and encourage more organizations to participate in cyber-security.

The specific objectives of this work therefore are to:

i. carry out a cost benefit analysis (CBA) of cyber security systems.
ii. formulate a mathematical model for CBA of cyber security systems.
iii. simulate the formulated mathematical model of cyber security systems using Java programming language.

III. METHODOLOGY

An extensive review of related literatures on Computer Networks and Communication, Risk Management Systems as well as Benefits and Costs analysis was carried out.

Contributory factors to cyber-crime were formulated and questionnaires administered to selected institutions of higher learning, banks, cyber cafés, offices of the Nigeria police, offices of the Nigeria Security and Civil Defense Corps, Law chambers, Law courts and several other selected Scenery. Confidential personal information will be supplied as respondents would be asked to specify their age, occupation and gender. The respondents were encouraged to be honest about their claims while items in the questionnaire involving some other internet technicalities were explained for clarity on the part of the respondents. Information gotten from the questionnaires was then analyzed using Statistical Package for Social Sciences (SPSS).

A. Background of the Research Area

Ondo, a state in Nigeria chosen as our case research area has an Area of about 15,500 km^2 (6,000 sq mi). It was created on 3rd February 1976 from the former Western State with Akure as the state capital. It has a Population of a total of 3,440,000 (2011 estimate, Federal Office of Statistics), and a density of about 220/km^2 (570/sq mi). The state contains eighteen Local Government Areas, the major ones being Akoko, Akure, Okitipupa, Ondo, and Owo. The majority of the state's citizens live in urban centers. The big government Universities in Ondo state are the Federal University of Technology Akure (FUTA), Akure and the Adekunle Ajasin University, Akungba/Akoko (AAUA). The ethnic composition of Ondo State is largely from the Yoruba subgroups of the Akoko, Akure, Ikale, Ilaje, Ondo, and Owo peoples. Ijaw minority (such as Apoi and Arogbo) and Ilaje populations inhabit the coastal areas; while a sizable number of the Ondo State people who speak a variant of the Yoruba language similar to Ife dialect reside in Oke-Igbo. These people are also Yorubas. Ondo State contains the largest number of public schools in Nigeria, over 880 primary schools and 190 secondary schools.

B. Sampling Population

The sampling population represents the population of the students in higher institutions of learning, Internet Service Providers, that is, managers of cybercafés as well as financial organizations, such as the united Bank for Africa(UBA), Guarantee trust bank(GTB), Diamond bank, Access bank, First bank, Enterprise bank, Fidelity bank and Eco bank. At least seventy (70) questionnaires were administered to these financial organizations, hundred (100) to higher institutions of learning, and about eighty (80) to internet service providers (i.e cyber cafés) making a total of two hundred and fifty questionnaires administered.

C. Method of Collecting Data for the Proposed Framework

A survey method was considered appropriate in helping to describe the patterns and the dispositional attitude of respondents to cyber-security. The choice of respondents

ISBN: 978-988-14047-1-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

was random but limited to internet users alone. To enable the collection of information, Interviews were conducted for selected I.T. personnel in the banking sector, cyber café managers, regular users of the Internet and students in some higher institutions of learning. Relevant open and close questions were asked so as to compare the cost they incure in trying to secure themselves on the Internet, and the benefits they expect. Responses from these categories of people were straight forward enough to help get the actual cost benefit analysis of cyber-security systems.

A two section questionnaire was designed to include all the information needed for the cost benefit analysis of cyber security systems. The various questions were designed to reflect the research objectives such as respondent's bio-data, understanding of cyber rime, strategies employed against cyber-crime, direct cost and indirect cost associated with each of the choice of cyber security strategy. The corresponding benefits associated with the choice of cyber security strategy such as the average user/ customer convenience for respective choice of strategy used against cyber-attack, various monthly budget and expenditure on cyber-crime, impact on IT and Non IT department. The questionnaire was tested for validity by administering a general interpersonal skill questionnaire on 10 bankers and 10 internet service providers and 10 university students. The aim was to establish a criterion validity rating between the budget and expenditure of financial organizations, internet service providers and university students on cyber security respectively.

IV. FORMALIZATION OF THE COST-BENEFIT ANALYSIS (CBA) PROCEDURE FOR CYBER-SECURITY SYSTEMS

There are several steps involved in carrying out Cost-Benefit Analysis. In order to enhance the Cost-Benefit Analysis of Cyber Security Systems, we modeled the various stages as follows;

Let the Total Proactive Cost, T_P be given as

$$T_P = \sum_{i=1}^{n} p_i \quad \ldots \quad (1)$$

Where *P* denotes individual Proactive Cost and let the Total Reactive Cost, T_R, be given as

$$T_r = \sum_{i=1}^{n} r_i \quad \ldots\ldots \quad (2)$$

Where *r*, denotes individual reactive cost

Let β and $f(\beta)$ represent Cost Benefit and Cost Benefit Decision Function respectively.

Therefore, the Cost Benefit β, is formalized as

$$\beta = T_P - T_r \quad \ldots \quad (3)$$

while, the Cost Benefit Decision Function$f(\beta)$, is formalized as;

$$f(\beta) = \begin{cases} \beta > 0, \text{ Then, the Reactive strategy } is\ a\ better\ approach \\ \beta = 0, \text{ Then either of the two approaches could be taken .} \\ \beta < 0, \text{ Then, the Proactive strategy } is\ a\ better\ approach \end{cases} \quad (4)$$

V. DATA ANALYSIS AND DISCUSSION

Our discussions on cyber security systems are in terms of a Net Present Value (NPV) or Cost-Benefit Analysis (CBA). Our framework should imply that the costs implication of cyber security should be compared to the expected benefits. Analysis of Cost comparison between present and absent Cyber security is performed as well as their direct costs and indirect costs otherwise known as tangible and intangible costs respectively. Analysis of the Questionnaire used to evaluate the cost benefit analysis is being performed using Statistical Package for Social Sciences (SPSS). Instead of investigating the probability of a future attack, this project work takes a step back to estimate a mathematical model for determining the costs of cyber security attacks both tangible and intangible costs.

A. Cost of Cyber Security

Several metrics have been proposed in previous literature to calculate and manage cyber security costs in general; however, because of the irregularity of computer software development and the evolving nature of hackers, the future of security attacks is unpredictable. These costs ranges from breach containment, crisis management, investigations and customer compensation, damaged system replacements, and other penalties. Therefore, in this work the focus is on the tangible and the intangible costs of cyber security which calls for a need to clarify the difference between the Tangible and Intangible costs associated with cyber security before.

B. Tangible Costs/ Direct Costs

Tangible costs or direct costs are costs such as involve financial losses and loss of assets. This represent the monetary value of all services, hardware, software and other resources expended in providing cyber security systems. In this work, the types of tangible cost evaluated are outlined as follows.

i. Average purchase cost of hardware device before cyber-attack.
ii. Average repair cost of hardware damage after cyber-attack.
iii. Average cost of software damage after cyber-attack.
iv. Average cost of software solutions before attack.
v. Average cost of software update after cyber-attack.
vi. Average cost of hardware maintenance.
vii. Average cost of software maintenance.
viii. Average cost of labor (local technical expert or expatriate).
ix. Average cost of Research & information gathering.

C. Intangible/ Indirect Cost of Cyber Security

Additional labor (wasted labor), downtime and business interruptions can be described as intangible cost incurred especially when there are cyber security breaches. Intangible costs should factor into investment decisions. Most times,

ISBN: 978-988-14047-1-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

they are not financial costs. For example, if an organization has a widely known breach, it could lose current or future customers because of the effects on its reputation. It could also suffer legal repercussions and further reputation damage if confidential information is compromised, particularly now that various state privacy laws force organizations to release information on breaches when private information is lost. Cyber security breach losses are becoming a significant component of companies' accounting records with implications from intangible costs such as reputational damage. Cyber Security cost can differ due to company size and industry type. In this work, the types of intangible cost evaluated are outlined as follows.

i. The effort or need for reactive labor after being proactive.
ii. Amount of resources (labor) required to respond quickly after a cyber-attack.
iii. Rate of data loss after cyber-attack.
iv. Average user/ customer convenience for respective choice of strategy used against cyber-attack.
v. Potential damage through cyber-attack to reputation.
vi. Rate of business interruption during a cyber-attack.

D. Cyber Security Strategies Employed by Respondents

Organizations and companies have different cyber security strategies. Based on research, it was discovered that these strategies generally range from proactive to reactive, where a proactive strategy implies that security compromises are anticipated and safeguards are built into the IT system to prevent them and a reactive strategy implies that an organization responds to known threats with typically established technologies so that security compromises can be addressed efficiently and effectively. Fewer security compromises resulted when an organization or company adopted a proactive strategy as opposed to a reactive strategy. During the interview process, respondents were asked to characterize their cyber security activities and strategies in terms of proactive or reactive. In some cases, an organization employed a cyber-security strategy with both proactive and reactive elements.

An important component of the implementation strategy cited by organizations that were interviewed was to what extent cyber security strategies should focus on preventive/proactive solutions versus reactive solutions. This logically raises the question: what is the optimal strategic mix of proactive versus reactive cyber security activities for an organization? Whereas a proactive strategy, in general, leads to fewer cyber security breaches, in some instances a reactive strategy may be more cost-effective. The adoption of a proactive versus reactive strategy has an impact on IT expenditures and overall business operations.

Table 1, provides an overview of the general cyber security costs and benefits as reported by respondents based on their choice of cyber security strategy (proactive and reactive), IT and Non IT impacts.

Table 1: overview of the costs and benefits of cyber security strategies as reported by respondents

Security Strategy	IT Impacts	Non-IT Impacts
Proactive	**Cost:** Cutting-edge hardware and software likely more expensive than well-established solutions.	**Cost:** User inconvenience.
	Cost: Information gathering, installation, debugging, and maintenance costs (labor).	**Benefit:** Regulatory and reputation benefits.
	Benefit: Decreased need for reactive labor.	**Benefit:** Fewer business Interruptions.
Reactive	**Cost:** Infrastructure (mostly labor) resources needed to respond quickly and effectively.	**Cost:** More events, and thus a likely increase in down time
	Cost: Resources (labor) needed to repair damaged systems and data.	**Cost:** Potential damage to reputation

In most instances, organizations that were interviewed discussed the effectiveness of the security strategy they employed, the advantages involved and the disadvantages equally. Generally, a larger percentage of them used at least one security strategy while some used both.

To guide the course of this study it is important to put the assumed impact of cyber security in perspective by attempting to find answers to the following research questions.

1. Are there gender variations in the interpersonal disposition of Nigerians who use cyber security techniques?
2. Are there factors influencing organizations' decision for specific cyber security strategies, if there are, what are they?
3. Is there any significant difference in the amount spent on reactive and proactive strategy?
4. Are there any organizations or individuals that are not cyber security conscious in this age?
5. What percentage of an organization's budget can be allotted to cyber security?
6. What are the factors influencing the share of IT cyber security expenditures?
7. What is Comparison between sources of cyber security investments within IT and Non-IT department of organizations**?**

Subsequent analysis provides answers to all the above questions.

ISBN: 978-988-14047-1-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

E. Descriptive Statistics of the Questionnaire

Table 2: Descriptive statistics of questionnaire.

SN	Description of Questionnaire	Number	Percentage
1.	Total Number of Questionnaires Distributed	250	100%
2.	Number of Questionnaires Received against (a.)	227	90.80%
3.	Number of Questionnaire Received from Banks against (b.)	68	29.95%
4.	Number of Questionnaire Received from Cyber Café against (b.)	63	27.75%
5.	Number of Questionnaire Received from Students against (b.)	96	42.29%

F. Gender Comparison of Respondents

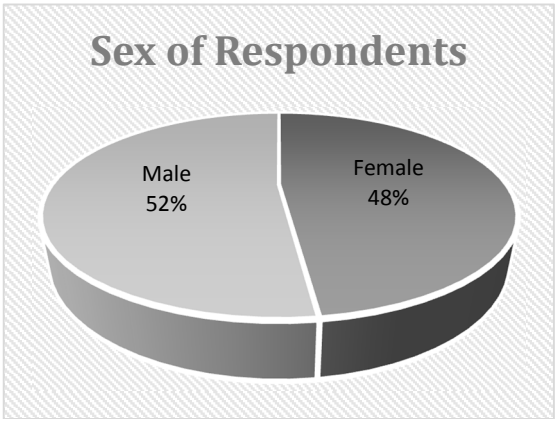

Figure. 1: Gender Comparison of Respondents

The pie chart in figure 1 shows that we discovered that the use of cyber security systems is not affected by gender factor, neither is the use of a particular method affected by it. Therefore, it cannot be concluded that a particular gender is more proactive in strategy or more reactive.

G. Statistical Analysis of the Cyber Security Strategies Employed among Organizations

Table 3: Statistics of the strategy employed against cyber attack

Cyber Security strategy	Frequency	%	Valid %	Cumulative %
Proactive Method Only	49	21.6	21.6	21.6
Reactive Method only	32	14.1	14.1	35.7
Both	116	51.1	51.1	86.8
None	30	13.2	13.2	100.0
Total	**227**	**100.0**		

Interviews showed that:

(i) Approximately 21.6% of all the respondents adopted the proactive strategy against cyber-attack.
(ii) Approximately 14.1% of all the respondents adopted the reactive strategy against cyber-attack.
(iii) Approximately 51.1% of all the respondents adopted both strategies against cyber-attack.
(iv) Approximately 13.2% of all the respondents adopted none of the strategies against cyber-attack.

H. Factors Influencing Organizations' Decision For Specific Cyber Security Strategies.

The interviews also included a discussion of what factors influenced organizations' decisions to adopt a specific security technology or to invest in the adoption of a new cyber security strategy. The following factors were most often cited:

(i) Likelihood to improve security: this factor was, not surprisingly, most often cited. The ability of the product or policy/procedure change to improve security, either to meet internal security objectives or to satisfy a government regulation, was very important to almost all respondents.
(ii) Ability to improve productivity: the second most important factor, cited by more than one-half of the interview participants, was the ability of the procedure to improve the productivity of users and/or cyber security staffs.
(iii) Ability to improve customer convenience: most respondents in various organizations have their customer convenience in high priority.
(iv) Elimination of potential damage through cyber-attack to reputation: Most organizations in the interview conducted would not want their reputation damaged through cyber security breach.
(v) Ability to reduce business interruption caused by cyber-attack: Most of the organizations interviewed reported that they would mostly not want any form of business interruption during their business hours, especially the financial institutions involved.
(vi) Rate of confidential information and data loss caused by cyber-attack: Private information to most organization should not be stolen, destroyed or exposed to unauthorized access. This therefore is a drive to ensure sound cyber security techniques are employed.

Proactive strategies have regulatory and reputational benefits, and because they are likely to lead to fewer events, can decrease business interruptions. However, interviews conducted on respondents said that proactive strategies can be restrictive. Close to one-third of the organizations interviewed said that user convenience was equally if not more important than security, which led them to use reactive strategies in some instances. In some organizations, management staff look to leverage a wide range of information and expertise when assessing cyber security threats and developing a cyber-security investment strategy. Such capabilities enable organizations with a more holistic view of cyber security to determine the appropriate level of security or due diligence and then have their IT staff develop

ISBN: 978-988-14047-1-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

the most cost-effective implementation strategy. In this way, organizations seek to minimize costs while achieving a desired level of security. This strategy will include a combination of proactive and reactive measures. Investments in cyber security are costly, as are repairs from breaches. Thus, an organization will select a cyber-security strategy that minimizes what it views as net costs. This can involve investing in both cyber security hardware and software and staff training, as well as modifying organizational operations that could increase day-to-day operating costs by restricting how IT systems can be deployed or how users can access/interact with IT systems.

I. Organizations and Individuals with no Cyber Security Strategy.

To answer question 5 of section (V) sub-section D asked earlier, on whether or not there are organizations with no particular cyber security strategy. Questions were asked respondents about the factors responsible for organizations or individuals not to adopt technologies, more than half of the respondents especially students in higher institutions of learning indicated each of the following factors (listed in order of the number of times each was mentioned, the first being the most frequent):

(i) disruption of users or cyber security staff productivity,
(ii) expense of the product,
(iii) too complicated and time consuming,
(iv) difficulty convincing management, and
(v) anticipated staff resistance.

Of particular interest is that disruption of user and/or cyber security staff productivity was cited most often by organizations as a reason why a certain technology, policy, or procedure was not adopted. This indicates a major barrier to the adoption of adequate security processes. Although organizations did not cite cost as an important factor when deciding to adopt a new technology, policy, or procedure, this factor was cited mostly by students.

Finally, organizations assess the effectiveness of their cyber security investments differently. Many rely on internal and external factors, and vulnerability tests to assess compliance with regulations and customer requirements, as well as whether the investments satisfy internal security goals.

J. Average Cyber Security Expenditure as a Percentage of I.T Budgets by Organizational Grouping

Table 4: average cyber security expenditure as a percentage of I.T budgets, by organization grouping

Industry	Percentage of IT budget
Banks	$\frac{(\sum W_{banks} + \sum X_{banks})}{(\sum Y_{banks} + \sum Z_{banks})} * 100\% = 63.86\%$
Universities	Not Applicable
Internet Service Providers (ISP) e.g. Café	$\frac{(\sum P_{isp} + \sum Q_{isp})}{(\sum R_{isp} + \sum S_{isp})} * 100\% = 64.41\%$
Total	64.14%

Let $\sum W_{banks}$ and $\sum P_{isp}$ be Proactive Average monthly Expenditure of IT department on cyber crime for banks and internet service providers respectively.

$\sum X_{banks}$ and $\sum Q_{isp}$ be Reactive Average monthly Expenditure of IT department on cyber crime for banks and internet service providers respectively.

$\sum Y_{banks}$ and $\sum R_{isp}$ be Proactive Average monthly budget of IT department on cyber crime for banks and internet service providers respectively.

$\sum Z_{banks}$ and $\sum Z_{isp}$ be Reactive Average monthly budget of IT department on cyber crime for banks and internet service providers respectively.

(i) On Cyber security expenditure as a percentage of IT budgets for banks, we have;

$$\frac{(900600 + 661700)}{(1221200 + 1225350)} * 100\% = 63.86\%$$

(ii) On Cyber security expenditure as a percentage of I.T budgets for Internet Service Providers, we have;

$$\frac{(590600 + 395800)}{(770100 + 761300)} * 100\% = 64.41\%$$

From the above analysis, it is concluded that organizations invest an average of 64.14% of their total IT budget on cyber security. The chart below also could help us decide whether an increase in the budget of an organization can result to a corresponding increase in the organizations' expenditure in cyber security or not.

ISBN: 978-988-14047-1-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

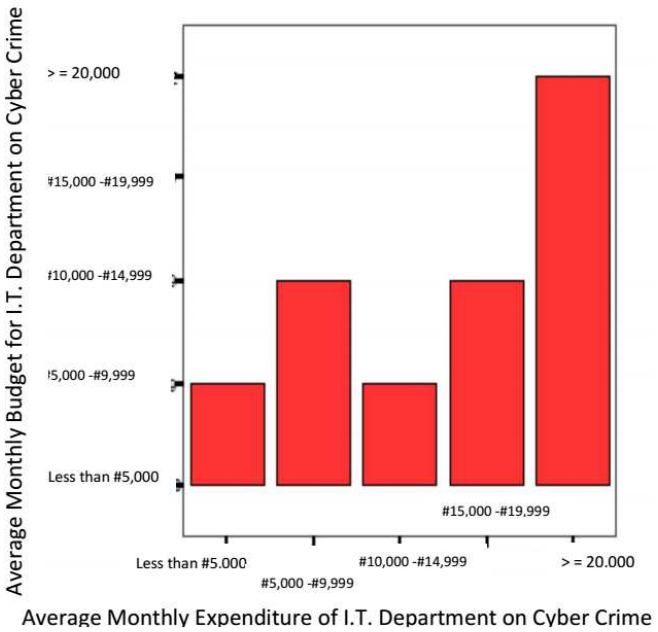

Figure 2: Average Monthly Budget against Average Monthly Expenditure

K. Factors Influencing The Share Of I.T. Security Expenditures

Based on interviewees' comments to the survey questions, discussions with numerous experts on cyber security trends and problems, and a review of the past literature, the following hypothesis is speculated and was tested by the correlation coefficient analysis below:

Hypothesis 1:

Null **:** Organizations with structured cyber security budgeting processes will not expend a larger share of their IT budget on cyber security.

*Alternate***:** Organizations with structured cyber security budgeting processes will expend a larger share of their IT budget on cyber security.

L. Correlation Coefficient Between Monthly Budget And Expenditure For I.T Department In Banks.

Table 5, shows the correlation co-efficient between monthly budget and expenditure for I.T. Department in banks.

Table 5: Correlation coefficient between monthly budget and expenditure for I.T. Department in banks.

		AVERAGE MONTHLY BUDGET	AVERAGE MONTHLY EXPENDITURE
AVERAGE MONTHLY BUDGET	Pearson Correlation	1	.615**
	Sig. (2-tailed)		.000
	N	227	227
AVERAGE MONTHLY EXPENDITURE	Pearson Correlation	.615(**)	1
	Sig. (2-tailed)	.000	
	N	227	227

** Correlation is significant at the 0.01 level (2- tailed).

Considering the bivariate correlation above, the null hypothesis is rejected because there is significant relationship between the average monthly budget for IT department and average monthly expenditure of IT department on cyber-attack as shown by the 0.615 value of the Pearson correlation coefficient. It can therefore be concluded that an increase in an organizations' budget would result in a corresponding increase in the organizations' budget for cyber-security. Consider also Fig. 3.

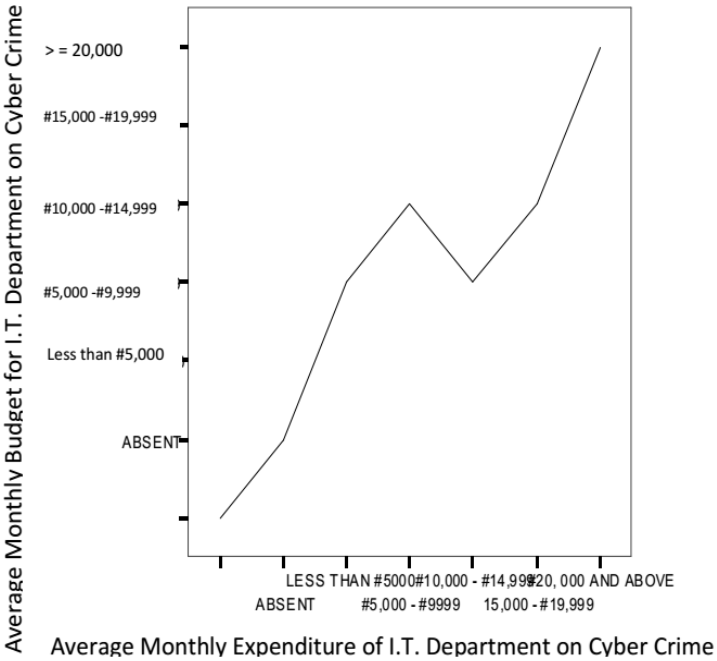

Fig 3: Average Monthly Budget of I.T. Departments against Average Monthly Expenditure of I.T. Departments on Cyber Crime

The first (Null) hypothesis reflects a good understanding of what takes place during a structured or systematic annual cyber security budgeting process. Such activities, within the organizations that we interviewed, are more deliberate and incorporate reasoned forecasts of security needs. These organizations are also relatively more proactive and anticipatory in their strategy toward cyber security.

The final (Alternate) hypothesis reflects the understanding that many cyber security compromises originate internally from employees and that more labor-intensive industries (e.g., financial services and universities) may be impacted more heavily by cyber security problems. Thus, an organization with value being generated in a more labor-intensive way will require greater cyber security investments.

M. Cyber Security Investments and Implementation Strategy

This approach analyzes the level or share of resources (budget) that an organization should or has available to invest in cyber security. In this scenario, a certain amount of money comes out of the organization's budget, and cyber security activities and purchases are determined by maximizing the use of available resources. This is the best approach in that it may not explicitly identify cyber security needs and thus could result in either an underinvestment or an overinvestment in cyber security.

ISBN: 978-988-14047-1-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

(i) Source of Cyber Security Investment Strategy in Financial Services (i.e. Banks)

Table 6: Source of Cyber Security Investment Strategy for financial sectors

	PROACTIVE METHOD		REACTIVE METHOD		
S/N	I.T	NON I.T	I.T	S/N	I.T
1.	₦32,700	₦17,400	₦19,500	1.	₦32,700
2.	₦82,500	₦48,000	0	2.	₦82,500
3.	₦12,500	₦46,000	0	3.	₦12,500
…	….	…	…	…	….
…	…	…	…	…	…
…	…	…	…	…	…
68.	₦12,000	₦14,000	₦4,500	68.	₦12,000
TOTAL	#1,221,200	₦1,048,500	₦1,225,350	TOTAL	#1,221,200

(a). Now, The average cyber security investment as a percentage of I.T budget is computed as:

$$= \frac{\sum \mathbf{PBIT_{banks}} + \sum \mathbf{REIT_{banks}}}{\sum \mathbf{IT\ Budget\ for\ Banks}} \times \mathbf{100}\%$$

Which is,

$$= \frac{\mathbf{₦1,221,200 + ₦1,225,350}}{\mathbf{₦43,172,00}} \times \mathbf{100}\%$$

that is

$$= \mathbf{56.67\%}$$

While,

(b) the Average cyber security investment as a percentage of Non I.T budget

$$= \frac{(\sum \mathbf{M_{banks}} + \sum \mathbf{N_{banks}})}{\text{Total Banks' Non} - \text{I. T. Budget}} \times \mathbf{100}\%$$

Which is,

$$= \frac{\mathbf{₦1,048,500 + ₦822,150}}{\mathbf{₦43,172,00}} \times \mathbf{100}\%$$

that is,

$$= \mathbf{43.33\%}$$

Where, $\sum M_{banks}$ denote the Proactive Average monthly Budget of Non-IT department on cyber-crime for banks, and $\sum N_{banks}$ stands for Reactive Average monthly Expenditure of Non-IT department on cyber-crime for banks.

Hypothesis 2:

Null: Organizations that have larger cost value of asset and information will not invest a larger share of their IT budget on cyber security.
Alternate: Organizations that have larger cost value of asset and information will invest a larger share of their IT budget on cyber security.

The null hypothesis above postulates that Organizations that have larger cost value of asset and information will not invest a larger share of their IT budget on security. This is tested using statistical analysis in table 5 and table 6 comparatively. The financial organizations invested a total IT budget and Non-IT budget of **₦4,317,200** on cyber security while internet service providers invested a lesser amount IT budget and Non-IT budget of **₦2,612,450** on cyber security. Therefore, the null hypothesis is rejected using the above statistical analysis because financial organizations have larger cost value of asset and information and as a result invest a larger share of their IT budget on cyber security compared to internet service providers (i.e banks).

(ii) Sources of Cyber Security Investment Strategy for Internet Service Providers

Table 7: Sources of Cyber Security Investment Strategy for internet service providers

	PROACTIVE METHOD		REACTIVE METHOD		
S/N	I.T	NON I.T	I.T	S/N	I.T
1.	₦64,200	₦27,600	₦7,500	1.	₦64,200
2.	₦94,200	₦38,200	₦9,000	2.	₦94,200
3.	0	0	0	3.	0
…	….	…	…	…	….
…	…	…	…	…	…
…	…	…	…	…	…
63.	₦17,500	₦3,800	₦10,800	63.	₦17,500
TOTAL	₦770,100	₦620,500	₦761,300	TOTAL	₦770,100

(a) Using values from Table 7, Average cyber security budget as a percentage of I.T budget can be computed as:

$$= \frac{(\sum \mathbf{R_{isp}} + \sum \mathbf{Q_{isp}})}{\text{Total I. T. Budget for Internet Service Providers (ISP)}} \times \mathbf{100}\%$$

Which is,

$$= \frac{\mathbf{₦770,100 + ₦761,300}}{\mathbf{₦2,612,450}} \times \mathbf{100}\%$$

that is,

$$= \mathbf{58.61\%}$$

(b) the Average cyber security budget as a percentage of Non I.T budget

$$= \frac{(\sum \mathbf{A_{isp}} + \sum \mathbf{B_{isp}})}{\sum \mathbf{Non - IT\ Budget\ for\ ISP}} \times \mathbf{100}\%$$

$$= \frac{\mathbf{₦620,500 + ₦460,550}}{\mathbf{₦2,612,450}} \times \mathbf{100}\%$$

ISBN: 978-988-14047-1-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

= **41.38%**

Let $\sum A_{isp}$ be Proactive Average monthly Budget of Non-IT Department on cyber-crime for internet service providers.

$\sum B_{isp}$ be Reactive Average monthly Expenditure of Non-IT department on cyber-crime for internet service providers.

(iii) Comparison Between Sources Of Cyber Security Investments In Organizations.

Table 4.8: Comparison between sources of cyber security investments within IT and non-IT Departments of Organizations.

S/N	INDUSTRY GROUP	WITHIN I.T.	WITHIN NON-I.T.
1.	**Banking**	**56.67%**	**43.33%**
2.	**Internet Service Providers**	**58.61%**	**41.38%**
AVERAGE TOTAL		**57.64%**	**42.34%**

The sources of cyber security investments strategies for most organizations emanate from both of their information technology and non-information technology departments. But in most cases, the I.T department invests the larger amount into cyber security systems. Compare the industry group in table 8, IT and Non IT budget for cyber security systems respectively.

N. Simulation Of The Formulated Mathematical Model

Our mathematical models for Total Reactive Cost and Total Proactive Cost, as well as those for decision making based on the Cost Benefit Function, as shown in equations (1), (2), (3) and (4), were simulated using Java programming language, into a software application, that will automatically carry out Cost-Benefit Analysis if the appropriate parameters (or values) are provided. Three major sectors, which includes, the Educational Institutions, The Financial Institutions as well as the Internet Service Providers were considered for information gathering on "the cyber security strategies" and "amount of costs incurred" while trying to protect their systems against cyber-attacks. From the information gathered, the following were deduced;

- Total Cost of Proactive Strategy for university Students = ₦ 3,339,200
- Total Cost of Reactive Strategy for university students = ₦3,125,050
- Total cost of Proactive Strategy for internet service Providers = ₦10,831,133
- Total cost of Reactive Strategy for internet service providers = ₦4,746,400
- Total cost of Proactive Strategy for financial institutions = ₦8,280,062
- Total cost of Reactive Strategy for financial institutions = ₦7,466,655

The Total Proactive Cost T_P, given as $\sum_{i=1}^{n} p_i$ would now be given as

$$T_P = \sum_{i=1}^{n} p_i = ₦\ 3,339,200 + ₦10,831,133 + ₦8,280,062 = ₦22,450,395$$

While, the Total Reactive Cost T_r, given as $\sum_{i=1}^{n} r_i$ would now be given as

$$T_R = ₦3,125,050 + ₦4,746,400 + ₦7,466,655 = ₦15,338,105$$

Now, our cost benefit in this case is the difference between the Total Proactive Cost minus The Total Reactive Cost. That is;

$$\beta = T_P - T_R$$

Which is;

$$₦22,450,395 - ₦15,338,105 = \mathbf{₦7112290}$$

This cost benefit value is quite high, and that, according to equation 4 means the Reactive strategy for cyber security systems is more beneficial and is a better approach.

The Models in this work were implemented into a Cost Benefit Analysis application. This application provides for automated Cost Benefit Analysis.

The CBA application allow us to automatically compare the amount expended on cyber security while using a particular strategy model with the amount budgeted while using the same strategy. Reports can be generated which will help users verify whether their current cyber security strategy (Proactive or Reactive strategy) is better or not.

VIII. CONCLUSION

In this work, cyber-security strategies were explicitly discussed. A survey and analysis of cyber security strategies as well as the various factors influencing the choice/use of any of them was also carried out. A mathematical model was formulated for Cost Benefit Analysis (CBA) of Cyber Security Strategies. The Model was also simulated using Java programming language majorly for the purpose of assisting users in carrying out the Cost and Benefit Analysis of their particular choice of cyber security srategy. The work can help decision makers to detrmine which of Proactive and Reactive strategy against cyber attack is a better approach, or if both Strategies can be deployed simultaneously.

REFERENCES

[1] Adeniran, A. (2008). The Internet and Emergence of Yahooboys Sub-culture in Nigeria. *International Journal of Cyber Criminology, 2(2), 368-381.*

[2] Cost-Benefit Analysis Guide for NIH IT Projects (1999). Center for Information Technology, National Institutes of Health.

[3] Lounge, O and Chiemeke, S. (2008). Cyber Crime and Criminality in Nigeria-What Roles are Internet Access Point in Playing?

[4] Wei, F. et al. (2001). Cost-benefit analysis for network intrusion detection systems.In Proceedings of the CSI 28th Annual Computer Security Conference.

[5] Yiseul , C. (2012). *Strategic Philanthropy for Cyber Security (An extended cost-benefit analysis framework to study cybersecurity).*