Int. J. Manag. Bus. Res., 1 (4), 221-230, Autumn 2011

Cyber Risk Exposure and Prospects for Cyber Insurance

[1]I. A. Adeleke, [2]A . Ibiwoye, [3]F. F. Olowokudejo*

[1,2,3] *Department of Actuarial Science and Insurance, University of Lagos, Nigeria*

ABSTRACT: This study draws attention to the ubiquitous and borderless nature of cybercrime. It examines the prospect of introducing customized cyber insurance policy in the Nigerian market. As secondary data was not available, the study conducted a survey by administering three sets of questionnaire to purposively selected top executives in four Trade Groups that rely heavily on Internet transactions for their operations. The study found that the rate of usage of the Internet and the attendant exposures to cyber-attacks among the various Trade Groups are quite high. Findings also show that the traditional policies have limitations with respect to protection against cyber risks and that there is a prospect for marketing a specifically designed cyber insurance policy in Nigeria.

Keywords: *Internet transactions, Trade groups, Cyber risk, Cybercrime, Cyber insurance*

INTRODUCTION

With a population of 136 million and an annual growth rate of 2.9% (UNFPA, 2003), Nigeria is the most populous country in Africa and the eighth most populous country in the World (Oxford Business Group, 2008). On the economic front, Nigeria is Africa's leading producer of crude oil. With over-dependence on oil, other sectors have been neglected. Agriculture that was, once, the mainstay of the economy has continued to rely on subsistence farming and has failed to keep pace with the rapid population growth. Thus, unlike many other oil-producing countries, Nigeria's per capita income of $2,300 (CIA, 2008) remains one of the lowest in the world. The human development index of 37.3 ranks Nigeria 80 th among 108 developing countries (Human Development Report, 2008). The outcome from these indicators is easily predictable: unemployment and widespread poverty. This probably explains the background for the pre-occupation of some of the youths with Internet crime, referred to locally as 'yahooyahoo' or '419'.

While the international community vacillates, more criminals are realizing that online crime can be lucrative, particularly in the light of the volume of commercial and personal information that are now being stored electronically (Kierkegaard, 2005). With increased sophistication in their activities, over the years, perpetrators now leave little in the way of evidence that can be used to track them (Aginam, 2008). So far, it is difficult to say if government's anticrime measures are working, as the latest global cyber-crime statistics, published by Internet Crime Report (2008), listed Nigeria in the third position among the top 10 perpetrators. In fact, recently, cybercrime attained such a huge dimension in Nigeria that government had to set up the Economic and Financial Crimes Commission (EFCC) in 2004. It is, therefore, expected that measures to control cybercrime or the severity of its impact, including that arising from letter fraud, will interest the international community.

Cybercrime is not constrained by physical boundaries or subject to import or exchange restrictions. Although it may have been conceived in a particular country, its effect extends far beyond the country of origin to any place on the globe. Its character is also anonymous (Kierkegaard, 2005) thereby facilitating a wide range of illegal and illegitimate activities (Moitra, 2005). Various steps have been taken by different governments to protect their citizens and their businesses from cyber risk exposure. Answers have been sought from diverse angles, including international collaborative efforts by way of

*Corresponding Author, *Email:adeibiwoye@yahoo.com*

international police. Unfortunately, the traditions of jurisprudence have become too varied for such a force to be effective (Grant-Adamson, 2004). Thus, in spite of these policing actions, cybercrimes persist.

Individuals and business organizations are, therefore, left with no other choice than to arrange alternative means of protection. This is usually pursued in one of two ways. The first is the technological approach, through which security measures to ward off intruders is put in place. The problem with this approach is that it appears the perpetrators' ingenuity soon puts them one step ahead of technology.

The other approach is to adopt risk management methods consisting of risk avoidance, risk assumption and risk transfer. Particularly because loss to a business organisation, following a cybercrime, can be devastating, it appears that risk transfer mechanism, the most popular method of which is insurance, is often the easiest option to adopt. While still on the insurance option, however, it has been realized that the traditional type of insurance policies that a firm can purchase may not suffice in a number of circumstances, as they may not capture the true costs of cyber-attacks (Gralla, 2001). There are, therefore, two immediate tasks. The first is to evaluate if, and to what extent, various Trade Groups engage in Internet transactions while the second is to examine the prospect of marketing an insurance product, specifically designed to cover cybercrimes. To the best of our knowledge, such a study has not yet been undertaken in Nigeria. This study attempts to fill the gap.

Literature Review

Although cyber space and the attendant cybercrime are relatively new phenomena, the literature on cybercrime is extensive. This, perhaps, reflects the multidimensional nature of the crime and the apprehension that, in reality, there may be no safe harbour from the crime (Bhasin, 2007). As reported by Gaudin (2002), attention to the endemic nature of the crime was brought by a U.S. Security Expert, Michael Vatis, who observed that, although cyber-attacks are of a limited duration, their impact on customer confidence is long lasting. To make matters worse, not only is it possible to perform all the kinds of traditionally accepted crimes with the aid of a computer (Gordon et al, 2003), criminals were, indeed, among the first to recognize, in cyberspace, the potential of a wide-open, sparsely populated, and poorly policed space (Grant-Adamson, 2004).

Thus, unfortunately, the fight against cybercrime is far from being won. Some analysts have offered some reasons for the apparent unprepared-ness of society and the world, in general, about how to combat cybercrime. According to Michael Vatis, mentioned in Gaudin (2002), too little attention and too few resources are devoted to cyber security. As explained by Longe and Chiemeke (2008), cybercrimes have been in existence for only as long as cyber space existed without giving a clue as to the types of crimes that are manifesting. This only became clearer about 1998 when technology companies began to partner with insurance companies in order to offer clients both technology services and first party insurance (Davis, 1998; Duvall, 1998; Nelson, 1998; Bolot and Lelarge, 2007).

But firms do not seem to be in a hurry to embrace insurance for protection. According to Holmes (2004), constrained by premium costs, firms usually put forth three arguments as reasons that influence their decision not to transfer risk. Firstly, firms may regard the possibility of risk from a software security attack as low; therefore, they take the view that they can assume the risk internally. Secondly, they deem that a catastrophic outcome has a low probability of occurrence; therefore they assume the risk. Thirdly, they assume that a security event over an insurable threshold will be unrecoverable and, therefore, they tend to regard insurance as not making economic sense. Other reasons identified as the major constraints of cyber insurance include lack of industry data on cyber-crimes and related losses, the ambiguous and volatile nature of cyber risk, high correlation of one type of cyber risk with another, lack of underwriting experience and lack of awareness (Gordon and Loeb, 2003; Bohme, 2005a; Karhade, 2005; Briody, 2007; Hauserman, 2007). Retrocession was not helpful as reinsurance companies, blaming what they termed global "cyber-hurricane," discourage primary insurance companies from underwriting the risks. Indeed, by January 2002, Bohme (2005b), citing CSO magazine, reported that primary insurance companies started to explicitly exclude cyber-risks from existing contracts.

In spite of these limitations, insurance still holds an advantage over other market based solutions, as there already exists a basic understanding of how an insurance product functions. Other techniques, such as taxation, have been seen to be subject to high

transaction and monitoring costs (Kesan et al. 2005). In addition to the ability to absorb the financial impact of security risks, Bohme (2005b) identified three other advantages of the insurance approach. They include differential premiums, quantification of security measures in monetary metrics and research and development of security technology. Other works, in a similar vein, include Gordon et al. (2003), Kesan et al. (2005), Daughtrey (2001), and Mader (2002). The outcome of a survey reported by Turney et al. (2005) indicates that about 25 per cent of businesses use some kind of insurance, possibly several insurance policies, including identity theft, internal fraud, sabotage, worms and viruses, to manage cyber security risk. The only shortcoming is that these conventional insurance policies were designed to cover the traditional perils of fires, floods, theft, liability, accident, injury and death. Since they were written before the advent of the Internet, they do not expressly cover new Internet risks (Majucaet al.2006).

RESEARCH METHOD

The nascent nature of cyber insurance in Nigeria suggests that there may not be enough published data to carry out a meaningful evaluation of its use as a means of protection against cybercrime. In the circumstance, we conducted a survey to obtain data from organisations that are identified as major users of the Internet and other electronic media for business transactions. In Nigeria, as in many other developing countries, there is a large informal sector; artisans, subsistence farmers, etc., that have little or no need of the Internet for their operations. This excludes them from the survey. In the formal sector, we again distinguish between the organised private sector and the public sector. Our survey was targeted at firms that operate in highly regulated industries, since research had shown that these are the firms that are more likely to adopt cyber insurance (Garg et al. (2003). Although the public sector also makes use of the Internet, in Nigeria, firms in this sector are not highly regulated. This had been one of the sources of the inefficiencies witnessed in this sector and the basis for government's recent reform actions. It is also envisaged that, government, which is the sole employer in the public sector, is able to absorb shocks better than corporate organisations. For these reasons, the public sector was excluded from the survey.

Data was gathered through the use of a questionnaire which was administered and collected within a period of two (2) years from January 29, 2009 to November 2, 2011. We then carried out a pilot study, which showed that in the organized private sector, banks, insurance companies, IT companies and Conglomerates are the Trade Groups that are highly regulated. The instrument used for the survey consists of three sets of questionnaire that are designed to examine different objectives of the study. The first is designed to find out if a company engages in Internet transactions and the length of time since it got involved. The next set of questions is designed to assess the level of preparedness of the various organizations in preventing cyber-risk incidents. Questions in this regard range from how the employees are groomed to recognize early signals of a cyber-attack, to taking other preventive measures necessary to forestall cyber risks in an organization. The third set is intended to evaluate the prospect of cyber insurance as a distinct insurance product. Some of the questions were adapted from the US Cyber Consequences Unit Security Check List (Bumgarner and Borg, 2007).

We used purposive sampling to collect the data since it is recognized that, oftentimes, it is neither feasible, nor practical, nor theoretically sensible, to do random sampling (Trochim, 2006). The procedure consists of selecting four key officers in each organisation whose portfolios deal with, or have oversight functions for, Internet transactions. Only organisations that have their headquarters in Lagos were selected. For banks, IT and Conglomerates, the sample includes the IT manager, the manager of the insurance desk, the marketing manager who relates to the public and the chief executive officer. For insurance, the list excludes an insurance manager, since such a position does not exist. After the 2004 bank recapitalisation, the number of banks in Nigeria reduced, first from 79 to 25, and, later, to 24 with the merging of IBTC and Stanbic banks. The number of insurance companies also shrank to 49 after the 2005 consolidation of insurance companies.

The questionnaires were administered in all the banks and insurance companies. 20 companies that engage mainly in IT were identified. Among the Conglomerates, 50 were picked from Nigeria Business Directory and Yellow Pages published by Nigeriagalleria (2007). In totality, 523 executives were interviewed. The number is determined by the peculiarity of the Nigerian business environment where

sizable commercial companies are few. In administering the questionnaires, we enjoyed considerable co-operation from the respondents as all the respondents completed the questionnaires. The non-responses observed in the completed questionnaires were handled by revisiting the respondents concerned.

The basic model we used for the study is Logistic Regression because the responses are in categorical form. Logistic Regression analyzes binomially distributed data of the form:

$$Y_i \sim B(n_i, p_i), \qquad for\ i = 1, \ldots, n$$

where the numbers of trials, n_i, are known and the probabilities of success, p_i, are unknown. The model proposes that for each trial there is a set of explanatory variables which can be thought of as being in vector X_i and the model therefore takes the form:

$$p_i = E\left(\frac{Y_i}{n_i} \middle/ X_i\right)$$

The logits of the unknown binomial probabilities are modeled as a linear function of X_i, as follows:

$$z = \log it(p_i) = \ln\left(\frac{p_i}{1-p_i}\right) =$$
$$\beta_0 + \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3 + \ldots + \beta_k x_k$$

Logistic Regression is useful in predicting the probability of occurrence of an event by fitting data to a Logistic curve. In Logistic Regression, the relationship between 'input', z, and the probability of the event of interest is described by a function such as (Klienbaum, 1974; Hosmer and Lemeshow, 2000):

$$f(z) = \frac{1}{1+e^{-z}}$$

The variable, z, is known as the logit and is usually defined as

$$z = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3 + \ldots + \beta_k x_k$$

Therefore, it follows that

$$f(z) = \frac{1}{1+e^{-(\beta_0+\beta_1 x_1+\beta_2 x_2+\beta_3 x_3+\ldots+\beta_k x_k)}}$$

The model also assumes that z is linearly related to the predictors.

RESULTS AND DISSCUSSION

An analysis of the responses from the survey shows that banks and IT companies seem to depend heavily on the Internet for their business transactions while Conglomerates and the Insurance Groups appear not to be totally dependent. Across all industries, majority of the respondents seem to agree that some of the operations their companies perform are done via the Internet. A related observation is that most of the respondents in Conglomerates, Insurance, and banking sub-sectors submit that cybercrime would spread and eventually affect their organisations. Only respondents from the IT sector appear to think differently. They think that some technology will be developed to effectively prevent cybercrime.

Respondents supplied different dates as the year that their firms began to offer services through the Internet. This obviously follows from the fact that each Trade Group is composed of many companies with different fortunes and different capabilities. All the same, for most respondents in the Conglomerate and Insurance sub-groups, 2005 was the year when their firms began to offer services through the Internet. For banks and IT sub-groups, most respondents believe that their companies began Internet operations in 2002. Other interesting results revealed by an analysis of the outcome of the survey are displayed in tables 1-3.

Respondents from the banking sub-group opine that banks have quite an exposure to cybercrime. This is understandable because Nigerian banks transact quite a number of their operations online. In contrast, the figure for Conglomerates is low. Again, this can be explained by the fact that the functions of buying and selling are rarely transacted online in Nigeria. Another noteworthy result is that over 80% of the respondents believe that cybercrime is more likely to be pushed from outside the organization. Only respondents from IT organizations think otherwise, which seems logical since the IT environment already poses, for the employee, the problem of moral hazard. The outcome for the second set of questionnaires is presented in table 2.

The results show that within the banking and IT groups, respondents agree that the various techniques used by the perpetrators of cyber crime are explained to employees clearly enough. They should, therefore, be able to recognize the early signs of the crime. In the Insurance sub-sector, this education is also relatively high but about a third of the respondents in the Conglomerate division believe that the level of

preparation of the employees to recognize the crime is not sufficient. The outcome for the third set of questionnaires is presented in table 3.

Table 1: Electronic transactions in percentages (*N* = 523)

Variables	Trade Group			
	Conglomerate	Insurance	Bank	IT
Does your company perform any of its operations via the Internet?				
Yes	53.3	80.0	100.0	100.0
No	46.7	20.0	0.0	0.0
If yes, when did the company start offering its services via the Internet?				
2,002	11.8	7.0	23.1	21.9
2,003	14.8	15.7	12.6	12.8
2,004	14.3	14.3	14.3	14.3
2,005	23.6	14.1	27.0	14.6
2,006	11.8	14.1	3.9	7.3
2,007	11.8	21.2	3.9	14.6
2,008	11.8	13.5	15.4	14.6
With the present increase in the rate of cyber crime worldwide, do you think your company is at risk?				
Yes	93.3	78.6	80.5	80.0
No	6.7	21.4	19.5	20.0
Has your company ever encountered any computer/cyber related crime?				
Yes	7.1	8.3	76.8	26.7
No	92.9	91.7	23.2	73.3
By which of the following methods do you think the crime is more likely to be committed				
Internal	9.1	10.0	17.6	54.5
External	90.9	90.0	82.4	45.5
If no, do you think cyber crime is likely to spread and eventually affect your company in future?				
Yes	53.3	57.1	37.8	63.6
No	46.7	42.9	62.2	36.4

Source: Survey data

Table 2: Assessment of preventive measures put in place in percentages (*N* = 523)

	Trade Group			
Variable	Conglomerate	Insurance	Bank	IT
Are various cyber-attack strategies described to employees in enough details and with enough variations, so that the employees would have a good chance of recognizing the early signs of such attacks and promptly report?				
Yes	66.7	93.3	100	100
No	33.3	6.7	0	0
Do employees know whom they should notify, both inside and outside the company in the event of an apparent attack?				
Yes	83.3	93.3	94.6	75
No	16.7	6.7	5.2	25
Are employees, with access to highly critical systems or facilities, provided with special access codes that would signal that they are acting under duress?				
Yes	58.3	73.3	97.5	68.8
No	41.7	26.7	2.5	31.3
Are automated detection systems in place that would raise silent, remote alarms, if the duress codes are used?				
Yes	60	64.3	100	68.8
No	40	35.7	0	31.3
Are there alternative channels of communication that can be utilized in the event of normal channels being compromised by removing them from the network?				
Yes	60	78.6	90.5	93.8
No	40	21.4	6.5	6.3
Do employees know how to isolate systems that have been compromised by removing them from the network?				
Yes	66.7	57.1	93	100
No	33.3	42.9	7	0
Are there plans for manually quarantining and monitoring systems that may have been contaminated with false information without shutting down?				
Yes	66.7	66.7	97.7	73.3
No	33.3	33.3	2.3	26.7
Is there a procedure for moving quarantine lines as better information about the possible contamination becomes available?				
Yes	63.6	86.7	100	58.3
No	36.4	13.3	0	41.7
Do employees know how to go about restoring compromised information systems to their last known good state?				
Yes	50	73.3	97.6	84.6
No	50	26.7	2.4	15.4
Is there a mechanism for retrieving last known state when that state is a considerable time into the past?				
Yes	83.3	26.7	92.5	30.8
No	16.7	73.3	7.5	69.2

Source: Survey data

Table 3: Prospect of Cyber Insurance Policy in percentages (*N* = 523)

Variables	Trade Group			
	Conglomerate	Insurance	Banks	IT
Are you aware of a computer insurance policy?				
Yes	53.3	86.7	94.7	92.3
No	46.7	13.3	5.3	7.7
Do you currently have an insurance policy covering your computer and cyber risks?				
Yes	53.3	66.7	91.9	84.6
No	46.7	33.3	8.1	15.4
If your answer to the previous question is yes, does your policy provide protection against all cyber risks?				
Yes	58.3	50	83.3	69.2
No	41.7	50	16.7	30.8
Are you satisfied with the level of cover by the policy?				
Yes	71.4	81.8	91.2	91.7
No	28.6	18.2	8.8	8.3
Does the policy have any limitations?				
Yes	28.6	77.8	62.9	83.3
No	71.4	22.2	37.1	16.7
Are you aware of Cyber Insurance policy?				
Yes	18.2	46.7	72.2	66.7
No	81.8	53.3	27.8	33.3
Do you have one?				
Yes	10	20	19.4	25
No	90	80	80.6	75
If no, are you willing to substitute it for your present policy, if it provides a wider cover and benefits?				
Yes	25	58.3	84.8	57.1
No	75	41.7	15.2	42.9
Are you willing to pay a cost slightly higher than the premium on your present policy, for cyber insurance policy with a more extensive cover?				
Yes	22.2	69.2	88.2	63.6
No	77.8	30.8	11.8	36.4

Source: Survey data

Table 3 shows that most of the respondents are quite aware of what computer insurance policy is about, except for those from Conglomerates who seemed to be somewhat less aware. Even though 53.3 per cent of the respondents in the Conglomerates sampled affirm that their companies have some form of insurance policy covering their computer and cyber risks, only 58.3 per cent of these believe that they are fully protected against all cyber risks. Only 18.2 per cent of the respondents from the Conglomerate group claims to be aware of cyber insurance policy. The percentage of respondents in the Insurance Group that claim to be aware of cyber insurance is surprisingly less than 50. This may suggest that the higher percentages recorded for respondents from banking and IT sub-groups reflect an awareness brought to them through other means different from the marketing efforts of the insurance companies.

Table 4 shows the results of the fitted Logistic models for each of the Trade Groups at 95 per cent significance level. It is instructive to note that all the variables are highly significant at the 95 per cent level. This is indicative of a positive relationship between the dependent variable and the explanatory variables. Specifically, sector by sector analysis indicates that the odd, that accompany that is satisfied with the existing computer policy will consider taking a cyber-insurance policy, is 0.775, while that of the insurance companies, that have other preventive measures in place, is 0.68. For, IT firms, the odd, that an IT company, that does Internet transactions will purchase a cyber-insurance policy, is 0.998, while the odd, that one that is satisfied with existing cover, would purchase cyber insurance, is 1.372. This, therefore, suggests that telecom companies that are satisfied with existing insurance policy, are more likely to purchase the cyber policy than those that just perform Internet transactions. In the case of banks, the odd that a bank that uses Internet transaction, would pick up a cyber-insurance policy, is 1.078. Banks that carry out Internet transactions are 4.32 times more likely to patronize cyber insurance policy than those that have had cases of cyber-attack and 3.27 more likely than those that had experienced a number of cyber incidents.

The odds ratios for banks that are satisfied with existing cover and banks that have other measures in place are 0.850 and 0.851 respectively. Finally, the odds ratio for Conglomerates that are satisfied with the existing cover is 0.82; the corresponding ratio for those having other measures in place is 0.819, while that for companies that have experienced cases of attack is 0.249. Conglomerates that are satisfied with the existing cover are 3.29 more likely to purchase a cyber-insurance policy than those that have preventive measures in place. Similarly, Conglomerates that are satisfied with the existing cover are 2.73 more likely to purchase a cyber-insurance policy than those that had experienced a number of cyber incidents.

CONCLUSION

The study revealed that the rate of Internet usage among the various Trade Groups sampled is quite high and this exposes them to various cyber-attacks. As these attacks can interrupt the smooth flow of business operations or even cripple a company completely, organizations need to protect their interests by transferring such risks to insurance companies. However, the study reveals a general realization among the different Trade Groups that the existing insurance policies have limitations where protection against cyber risks is concerned. It also reveals that they are willing to pay a higher premium than that being charged by the existing policies so as to avail them of insurance specifically designed to cover cyber risks, if such a policy can be put in place.

It is, therefore, obvious that the unavailability of the cyber insurance policy in the Nigerian insurance market has contributed largely to why most companies do not have this cover. But, perhaps, the most revealing finding is that, even within the insurance industry, which is supposed to produce the policy, awareness of the existence of cyber insurance is very low. In general, awareness campaign of cyber insurance should be embarked upon with special attention given to Conglomerates.

RECOMMENDATIONS

Although cyber insurance provides the widest cover against cyber risks, it has not taken firm root yet in Nigeria because no insurance company offers the

Table 4: Logistic Regression predicting patronage of Cyber Insurance policy among different Trade Groups (*N* = 523)

Variables	Odd ratios			
	Conglomerate	Insurance	Banks	IT
Internet transaction	0.315*	0.317*	1.078**	0.998*
Satisfaction with existing cover	0.82**	0.775**	0.85**	1.372*
Availability of preventive measures	0.819**	0.680**	0.851**	0.413*
Past experience	0.249*	0.106	0.250**	0.423*
Number of incidence	0.318*	0.411*	0.330*	0.311*
R^2	0.400	0.536	0.884	0.100

*p<0.05 **p<0.01

cover. Insurance companies might be shying away from providing the cover due to inadequate market research and lack of know-how in new product development, as well as lack of relevant underwriting experience. These are areas that should interest the Nigerian Insurance Association (NIA) and the National Insurance Commission (NAICOM) at one level and the Insurance companies, themselves, at the corporate level. Insurance companies should invest in new product development and relevant training for staff. On the part of reinsurance companies, they can serve as buffers by providing knowledge and by increasing the capacities of ceding companies.

Especially because the level of cybercrime is high, it may not suffice for a country to simply adapt the approach already in use in other countries. In order to avoid an experience similar to that witnessed during the introduction of medical insurance scheme in Nigeria (Ibiwoye and Adeleke, 2007), there is need for a home grown cyber insurance cover which will take the peculiarities of the Nigerian environment into consideration.

To overcome the problem of paucity of actuarial data on which to base premium rates (Briody, 2007), insurance companies may, for a start, base their rates on existing theft policies and revise as experience prescribes. All these will require committing a considerable amount into cyber insurance research. The funding for such a research can be tax deductible from the profit of registered insurance companies. Restriction can be placed to limit the companies that would market the product to those that are prepared to embark on intensive staff training in cyber risk underwriting. This is important because cyber risks tend to be highly correlated with one another (Bolot and Lelarge, 2007) and underwriting the risks will, therefore, require more than the ordinary vigilance of a seasoned underwriter.

Since the study shows that companies, irrespective of Trade Group, that have existing insurance policies in place, are more likely to embrace cyber insurance, promoting cyber insurance can begin in earnest by introducing the policy to a prospect, who is at the point of purchasing other conventional policies. It could take the form of an explanation of the features, costs and, most importantly, benefits of the cyber insurance policy over other already existing policies.

In spite of the efforts companies put into preventing cyber- attacks, the risks of losing business or reputation still remain. Such residual risks can be covered by cyber insurance, which our results have shown to be desirable, especially in private sector organisations that use electronic information intensely and that are highly regulated. The benefit of cyber insurance however, extends beyond the highly regulated industries. If it works for regulated industries the effect will cascade down to the public sector and ultimately the informal sector. It may take the form of an offshoot of the very nature of the practice of insurance. By this, prospects may need to meet certain eligibility conditions in order to benefit from reduced premium. This will encourage the citizens to be more cyber security conscious and this will frustrate the perpetrators. With cyber criminals having difficulty breaking-in, as a result of the self-insurance that the foregoing implies, cybercrime will become unattractive. As premiums reduce, more organisations and individuals can be expected to pick up their own cyber policies.

REFERENCES

Adeloye, L. (2008). How to Guard Against Internet Fraud. *Punch*, (November 9), p. 4.

Aginam, E. (2008). Hackers and Nigeria Vulnerability to Cyber Terrorism. Vanguard, Available: http:// www.vanguardngr.com/ content/view/ 17676/51 (September 24, 2008).

Aun, S. L. Y. (2005). An Introduction to Cybercrimes: A Malaysian Perspective. Available: http://www.mae/e.net/ articles/ekom2005.pdf (February 6, 2012).

Bhasin, N. K. (2007). Journey of Indian Payment Systems – On Move. Paper presented at Bank net India's Third Conference on Payment Systems in Banks, Mumbai.

Bohme, R. (2005a). Vulnerability Markets: What is the Economic Value of a zero-day exploit, Proceedings of the 22 nd Chaos Communications Congress, Berlin, Germany.

Bohme, R. (2005b). Cyber-Insurance Revisited, Workshop on the Economics of Information Security (WEIS), Kennedy School of Government, Cambridge, MA.

Bolot, J. and Lelarge, M. (2007). A New Perspective on Internet Security Using Insurance. Available: http:// hal.inria.fr/docs/00/17/94/79/PDF/cyber-surv.pdf (March 24, 2009).

Briody, D. (2007). How to hedge your cyber risk. Available: http://www.inc.com/magazine/20070401/technology-insurance_pagen_2.html (January 29, 2009).

Bumgarner, J. and Scott B. (2007). The US-CCU Cyber-Security Check List. Available: https:// www.bhconsulting.ie/US_CCU%20Cyber-Security%20Check%List%202007.pdf (April 8, 2008).

CIA, (2008). The World Factbook – Nigeria. Available: https:/ /www.cia.gov.library/publications/the-world factbook/ geos/ni.html (May 28, 2008).

Daughtrey, T. (2001). Costs of Trust for E-Business: Risk Analysis Can Help E-Businesses Decide Where

Investments in Quality and Security Should Be Directed, *Quality Progress*, 10, pp. 38-43.

Davis B. (1998). Cigna Offers Anti-Hacker Insurance. Available: http://www.techweb.com/wire/story/TWB 19981005S0010 (April 8, 2008).

Duvall M. (1998). Big Blue to Offer Hacker Insurance Services, ZDNet. Available: www.citebase.org/ abstract? (April 8, 2008).

El-Guindy M. N. (2008). Cybercrime in the Middle East. Available:http://www.ask-pc.com/lessons/ CYBERCRIME-MIDDLE-EAST.pdf

Garg, A., Curtis, J. and Halper, H. (2003). Quantifying the Financial Impact of IT Security Breaches, *Information Management and Computer Security*, 11 (2), pp. 74-83.

Gaudin, S. (2002). Security Expert: U.S. Companies Unprepared for Cyber Terror. Available: http:// itmanagement.earthweb.com/secu/article.php/1429851, (April 25,2008).

Gordon, L. A., Loeb, M. P. and Sohail, T. (2003). A Framework for Using Insurance for Cyber Risk Management, *Communications of the ACM*, 46 (3), pp. 81-85.

Gordon, L. A. and Loeb M.(2003). The Economics of Information Security Investment, *Journal of Computer Security*, 11 (3), pp. 431-448.

Gralla, P. (2001). Insurance for Cyber Attacks has yet to Catch on. Available: http://www.cio.com/artic1e/30742/ Insurance for Online Attacks Has Yet to Catch on? (April 10, 2008).

Grant-Adamson, A. (2004). *Cyber Crime*, Broomall, Mason Crest Publishers Inc.

Hauserman, S. (2007). The CIP Report, Available: http:// www.cipp.gmu.edu.critical Infrastructure Protection Program, 6, pp2-9, (April 12, 2008).

Holmes, T. E. (2004). Cyber Insurance May Save Your Business if Digital Disaster Strikes. Available: http:// www.mozilla.org (April 10, 2008).

Hosmer, D. W. and Lemeshow, S. (2000). *Applied Logistic Regression*, New York: John Wiley and Sons.

Human Development Report, (2008). Nigeria: The Human Development Index – Going Beyond Income. Available: http://hdrstats.undp.org/countries/country_fact_sheets/ ctyfs_NGA. html (May 28, 2008).

Ibiwoye, A. and Adeleke, I. A. (2007). The Impact of Health Insurance on Health Care Provision in Developing Countries, *Ghana Journal of Development Studies*, 4 (2), pp. 49-58.

Indian Express (2009). India Emerging as a Major Cybercrime Centre: Study. Available: http://www.indianexpress.com. (February 6, 2012).

Internet Crime Report Center, (2008). The 2008 Internet Crime Report. Available: http://www.ic3.gov/media/ annualreport/2008_IC3Report.pdf (May 24, 2009).

Karhade, P.(2005). Security of Information Technology Assets and the Diffusion of Cyber Insurance. Available: http://www.Sqp .asg/pub/qualityprogress/past/l 00 1/qp 1001 daughtry.org (April 7, 2008).

Kesan, J. P., Majuca, R. P. and Yurcik, W. J. (2005). *The Economic Case for Cyber insurance, Securing privacy in the Internet Age*, Stanford University Press, p. 7.

Kierkegaard, S. M. (2005). Cracking Down on Cybercrime Global Response: The Cybercrime Convention, *Communications of the IIMA*, 5 (1), pp. 12-14.

Klienbaum, D. G. (1974). *Logistic Regression: A self-learning Text*, New York: Springer-Verlag.

Kumar, N. (2010). Africa Could Become the Cybercrime Capital of the World. Available: http://www.psfk.com/ 2010/04 (February 7, 2012).

Longe, O. B. and Chiemeke, S. C. (2008). Cyber Crime and Criminality in Nigeria: What Roles are Internet Access Points in Playing? *European Journal of Social Sciences*, 6 (4), pp. 132-139.

Mader, B.(2002). Demand Developing for Cyber-insurance.*Business Journal of Milwaukee*. Available: http:/ /biziournals.com/Milwaukee/stories/2002/10/14/ focus2.html? (April 6, 2008).

Majuca, R. P., Yurcik, W. J. and Kesan, J. P. (2006). The Evolution of Cyber insurance, ACM Computing Research Repository (CoRR) Tech. Report cs. CR/0601020

Moitra, S. D. (2005). Cyber Security Violations against Businesses: A Reassessment of Survey Data, Indian Institute of Management Working Paper Series, No. 571.

Nelson, M. (1998). ICSA Insures Against Attacks by Hackers, *Infoworld*, (September 25, 1998).

Nigeriagalleria, (2007). Nigeria Business Directory and Yellow Pages. Aavailable: http://www.nigeriagalleria.com/ Manufacturing_and_Production/Conglomerates_g.html (February 6, 2008).

Nkanga, E. (2008). Nigeria: Combating Cyber Crime Menace in Nigeria, *ThisDay*, April 16, 2008. Available: http:// allafrica.com/stories/200804170519.html (October 31, 2008).

Oxford Business Group,(2008).Nigeria – Country Profile. Available: http//www.oxford businessgroup.com/ country.asp?country=70 (April 25, 2009).

Poku, O. N. O. (2011). Cybercrime in Africa, a Stalemate to economic Development. Available: http:// www.allwestafrica.com/180620119225.html. (Feb 6, 2012).

Timbuong, J. O. (2011). Malaysia: Cybercrimes Continue to Rise. Available: http://www.apecdoc.org/site/malaysia/2011/ 09/26/cybercrimes-continue-to -rise. (February 6, 2012).

Turney, J. T., Steed K. and Guimaraes, E. (2005). Cyber Security Insurance: Managing Risk in the Digital Age, Diamond Security Solutions. Available: http://itom.fau.edu/ jgoo/fa05/ISM4320/DSS.pdf (April 10, 2008).

UNFPA, (2003). Available: http://Nigeria unfpa.org/ aboutus.htm (May 24, 2009).

Trochim, W.M. K.(2006). Research Method Knowledge Base. Available: http://www.socialresearchmethods.net/ kb/statinf.php, (May 14, 2008).

Wharton Scholl (2012). In the Middle East Cyberattacks are flavoured with political rhetoric. Available: http:// knowledge.wharton.upenn.edu/arabic/article.pdf (February 6, 2012).