J Communication, 8(2): 136-140 (2017)
DOI: 10.31901/24566586.2017/08.02.221

Analysis of Cyber-security Benefits on Cyberspace in Nigerian Insurance Companies

Oluwatosin O. Bamigboye[1], Olushola F.Olawuyi[2] and Rasheed A.Tomori[3]

[1]Department of Computer Science, University of Fort Hare. South Africa
[2]Centre for Open and Distance learning, University of Ilorin, Nigeria
[3]Computer Services and Information Technology, University of Ilorin, Nigeria
E-mail: [1]<201614053@ufh.ac.za >, [2] <festusshola@yahoo.com> and
[3]<tomorirasheed@yahoo.com>

KEYWORDS Cyber Security. Cyberspace. Insurance. Information Communication Technology. and ANOVA

ABSTRACT The innovation of the information and communication technology which has produced the Internet to connect the whole world as a global village has been seen as a vital aspect of our daily lives. Many organizations are now using the Internet with computer network for various activities and without doubt insurance sectors have also benefited tremendously from various Internet advantages and also with several benefits derived from using the cyber space to manage the online platform (website). Various studies have shown that the gravity of online attack is very costly if security attention is not given to the cyber space immediately. This research work will analyze various benefits of cyber security and the risks involved if security of the online platform is neglected. A research instrument (questionnaire) was distributed among the sixty-two (62) registered Nigeria insurance companies seeking their opinions on six (6) benefits of the cyber-security, after which a regression analysis was performed to justify their responses using a statistical software package.

INTRODUCTION

The introduction of the information technology without any doubt has made the Internet a major component of the modern economy. The development of the Internet and communication systems started with the new era of cyber movement that has fundamentally changed the way of work of the governmental and non-governmental organizations. People, governments, and most of the firms rely on Internet for their business and this reliance has caused the developed nations more risks through cyber threats (Li et al. 2017). Lots of advantages like connectivity to different online applications that are so strategic to many companies, individual users, and governments sectors with others services offered through the Internet including the network infrastructure with online users are all subjected to various Internet threats, which include hacking, service denial attacks, various kinds of intrusions, eaves-dropping, spams, worms and viruses (Shafqat and Masood 2016). In other words, to reduce or protect completely from these threats proactive measures like implementing defense mechanism such as, integration of anti-spam software, intrusion-detection systems and firewalls on the networks or even on the web platform of each organization is very necessary (Dean 2013). Due to this development, it is advised to various entities (enterprises, individuals and operators) that they should use the Internet services to provide a protection mechanism on their online intellectual property like the website and other online infrastructures including various services rendered or delivered through their online platform against the threats of cyber-attack (Kasemsap 2017). Therefore, there are risks associated with online platform which must be avoided, there must be acceptance of the threat with the loss that occurs, self-protection and risk mitigation and finally transfer of the threat to another party. Therefore, various entities have so far considered those risks which have resulted in the development and deployment of massive collections of different applications to detect the threats with the anomalies, and also protect the online infrastructure and the users from the destruction of those anomalies (Baldwin 2017). Security threats are very real and risk factors are higher ever than today in information centric and interconnected world (Patrick and Fields 2017).

Literature Review

Information and Communication Technologies (ICTs) have become an essential part of our daily lives. Boes and Leukfeldt (2017) have reported that Internet which is a major product of the ICT has been identified with lots of advantages from the users while the main challenge of this great innovation is still the issue of security which is affecting almost all the Internet users, including various sectors in the world at different levels. Brenda (2014) also reported that the evidence of this was predicted in a study which clearly shows that the world population of the Internet users will be seventy percent in the year 2015 which means according to this study that 70 percent of the users using the Internet will be facing challenges of Internet securities in the affirmation year. That is why security is now seen as an important measure in every area of our endeavors. Due to the advent of Internet, cyber security has become a solution or counter-attack mechanism to fight several activities happening in the cyberspace these days. Similarly, also reported by Ögütçü et al. (2016), cyber threats continuously increase with the adventures of technologies and the legal boundaries related to the privacy of personal information and its use by the corporations are not clear and are often subject to legal interpretation. The only major problem faced by the computer users and many establishments is the issue of security. Meanwhile, security history has allowed for arrival of security technology. Internet structure allows for several cyber threats to happen on different online platforms but understanding the attack method and taking the appropriate security measures can reduce damage caused by the online attack into a zero level (Rajra and Deepa 2015). Protection of a cyber-threat in managing sensitive information on the cyberspace must be an ultimate priority of all sectors. Many organizations that understand this, secure their businesses from Internet hackers through the means of encryption mechanisms and network firewalls. This is because damages implication of the cyber-attacks are so costly. Studies have clearly shown that the resolve time of cyber-attack is not less than 32 days with a total average cost of affected companies being over $1 million during the period of the 32 days (Pawlak and Wendling 2013) due to these costly damages of the cyber-attack as proved in a study through a survey on a cybercrime of United States companies in year 2013.

Damages of cyberspace of an organization resulting due to cyber-attack can be grouped into several forms, showing the extent to which cyber threat deserves to be prevented at a greater consideration than focusing on data disruption (Cap 2017). Where a cyber-attack affected an organization that depends solely on Internet for their financial activities, the violence may be felt as greatly as attacking the organization itself (Olson and Wu 2015). Cyber-attacks are currently becoming great threats that are becoming dangerous on the Internet and causing lots of devastation to various organizations, regardless of the size of the sector. Government of United Kingdom's Annual Rupture Report indicates that 81 percent of the large organizations and 60 percent of small organizations suffered a security rupture in 2014 as reported by Olson and Wu (2015). Information security has been given high attention due to the rapid development and widespread use of computers and communication networks which are not only applied to the military and diplomatic fields but have affected every aspect of people's lives (Walters 2014). In general, creating and evaluation of different protocols like data confidentiality, integrity, authentication, and non-repudiation that can overwhelm the influence of the cyber enemies which are associated with information security should be given proper attention (Agrawal et al. 2014). Personal and security sensitive information losses resulting from cybercrime, include online identity theft or usurpation financial fraud, stalking and blackmail (Al-Daraiseh et al. 2014; Reyns and Henson 2015).

Problems Statement

The introduction of the online security mechanism as a defense tactic to fight against cyber-attacks facing many organizations including insurance sector of this great nation has been seen as a significant innovation. This study weighs some of the advantages of cyber security over the disadvantages as mentioned by some of the organizations and through proper analysis it was proved that the benefits like protection of computers from being hacked, provision of privacy to the Internet, reduction in the grate of computer freeing and crash, protection of data against cyber theft, protection from spyware and com-

munication encryption over the following disadvantages like high cost of cyber security integration, difficulty in configuring some security appliances like firewall, updating problems of some security software and lastly some company said security software affect the performance of their computer system. Meanwhile, most of the previous researchers in this context have also confirmed lots of benefits of cyber-security on the online platform that overweighs its disadvantage because the implication of the damages is so costly.

Purpose of the Study

Aim of the study is to analyze cyber security benefits for the protection of cyber space of Nigeria insurance companies through a survey.

Research Objectives

1. To determine truly if cyber security protect the computer system from the hackers
2. To determine if cyber security provides privacy to Internet users
3. To determine if cyber security reduce computer from been freeing and crash
4. To determine if cyber security protect data against cyber theft
5. To determine if cyber security protect the system from spyware and other unwanted programs
6. To determine if cyber security provide communication encryption

Research Questions

This research seeks to answer following questions using cyber security benefits

1. Can cyber security protecting computer system from being hacked?
2. Can cyber security provides privacy to Internet users?
3. Can cyber security reduce computer system from been freeing and crash?
4. Can cyber security protect information data against cyber theft?
5. Can cyber security protect computer system from spyware and other unwanted programs?
6. Is it really true that cyber security provide communication encryption?

METHODOLOGY

The research work was conducted in a registered insurance company in Nigeria. Qualitative approach was used through survey questionnaires which were administered to a sample of 62 companies using sampling technique. Returned questionnaires were 58 which show response rate of 93.5 percent. A data representation was done using bar chart with regression analysis, qualitatively done using independent and dependent variable through the SPSS software

Research Design

The technique of this research work is proving the usefulness of cyber security on the cyberspace for insurance sectors using a well-structured questionnaire as an instrument for the collection of data. The population of the study consisted of 58 registered insurance companies in Nigeria who are aware or not on the advantages of security of the cyberspace. Approach used for the data collection was a questionnaire which served as an instrument in seeking opinion of the insurance company based on their awareness level on cyber security benefits. The data analysis was done based on 58 valid questionnaires that was returned and administered for the survey. A graphical representation was done using regression analysis through the SPSS software to prove various benefit of cyber-security based on each company perception.

RESULTS

Research Hypothesis

There is no level of significance between cyber security for insurance company and its benefit derived (Table 1).

The multiple regression of the cyber security for insurance company indicated that regression coefficient (R squared) is .96 percent. This shows that 96 percent of the variation in cyber security for insurance company is accounted for by the benefit it's derived.

In Table 2, the regression test carried out shows that all the benefits derived can significantly influence cyber security for insurance company. This is because the calculated F-val-

Table 1: Relationship of cyber security for insurance company and its benefit derived

Model Summary				
Model	*R*	*R square*	*Adjusted R square*	*Std. error of the estimate*
	.984[a]	.968	.964	.10538

Table 2: ANOVA

Model	*Sum of squares*	*df*	*Mean square*	*Fc*	*Ft.*
Regression	17.219	6	2.870	2.5416	3.00
Residual	.577	52	.011		
Total	17.797	58			

ue 2.5416 is greater than the table F-value 3.00. Therefore null hypothesis was rejected and it could be stated that significant relationship among cyber security for insurance company and the benefits it's derived

Table 3, shows that the coefficient of contribution of cyber security protects computer from being hacked is -.089, cyber security provides privacy to the Internet user contribution is -.135, cyber security reduces computer freezing and crash contributions is -1.124, protection of data from cyber security thefts contribution is 1.350, Protection of system against spyware and other unwanted program contribution is -.028 and communication encryption contribution is -.064. This indicates that protection of data from cyber thefts contributes more of cyber security to the insurance company than other benefits derived.

DISCUSSION

The outcome of the study through cyber-security benefits has clearly shown high level of significance based on respondents' responses in integrating cyber security on their online platforms of all the insurance company in the country. The result of the analysis performed from this study on benefits of cyber-security has shown and proved high level of usefulness of cyber security. It also showed through the ANOVA test that the calculated value for F value 2.5416 is greater than the F value 3.00 which makes the hypothesis null rejected which significantly influences cyber security for insurance companies. The finding is in the line as reported by Boes and Leukfeldt (2017) that Internet which is a major product of the information communication technology has a lot of advantages and disadvantages for the users while the main challenges of this great innovation are still the issues of security which are affecting the Internet users, including various sectors in the world at different levels of business. Another study (Brenda 2014) also reported that 70 percent of Internet users will be increasingly affirmative in years to come and face security challenge as well.

CONCLUSION

Based on this point and the response attitude of insurance companies toward cyber-security benefits on the cyber space, it can now be concluded that if more or better awareness is

Table 3: Coefficients[a]

Model	*Unstandardized coefficients*		*Standardized coefficients*	*T*	*Sig.*
	B	*Std. error*	*Beta*		
(Constant)	4.231	.451		9.379	.000
Cyber security protects computer from being hacked	-.089	.009	-.317	-10.354	.000
Cyber security provides privacy to the Internet user	-.135	.020	-.312	-6.839	.000
Cyber security reduce computer freezing and crash	-1.124	.138	-.910	-8.149	.000
Protection of data from cyber thefts	1.350	.069	2.175	19.508	.000
Protection of system against spyware and other unwanted program	-.028	.005	-.165	-6.015	.000
Communication encryption	-.064	.010	-.180	-6.368	.000

given to the insurance sectors, the acceptance of security integration will be greatly accepted and this will make Nigeria insurance sector meet up with their counterpart in the global world.

RECOMMENDATIONS

At this point the researchers' recommendations on this research work to all insurances companies and other IT firm is that they should all embark on a risk management and also provide adequate measures in tackling the problems of cyber-attacks instead of waiting for the damages to occur and now acting on it because is better to prevent from been affected than cure. The researchers' recommendations can still be further given using security model which is to prepare, protect, detect and improve. If this model can be followed adequately by insurance sectors and others organizations using the Internet for transaction at the level of attack by the cyber attackers will be prevented completely. Constant training on the use of ICT, Cyber-Security, and Security attack needs to be given more attention by all organization and better awareness on cyber security by the government on the risk management to all sectors.

REFERENCES

Agrawal Vikas, Agrawa Shruti, Deshmukh Rajesh 2014. Analysis and review of encryption and decryption for secure communication. *International Journal of Scientific Engineering and Research (IJSER),* 2(2): 1-3.

Baldwin A, Gheyas I, Ioannidis C, Pym D, Williams J 2017. Contagion in cyber security attacks. *Journal of the Operational Research Society*, 68(7): 780-791.

Brenda KW 2014. The role of psychology in enhancing cyber security. *Cyber Psychology, Behavior, and Social Networking,* 17(3): 131-132.

Boes S, Leukfeldt ER 2017. Fighting cybercrime: A joint effort. In: *Cyber-Physical Security.* Springer International Publishing, pp. 185-203.

Cyber Resilience - The Cyber Risk Challenge and the Role of Insurance. From <https://www.theoroforum.org/wp-content/uploads/2015/01/Cyber-Risk-Paper-Version/24-1.pdf>

Cano J, Hernández R, Ros S 2014. Bringing an engineering lab into social sciences: Didactic approach and an experiential evaluation. *IEEE Communications Magazine,* 52(12): 101-107.

Cap P 2017. Technological discourse: Threats in the cyberspace. In: *The Language of Fear.* UK: Palgrave Macmillan, pp. 53-66.

Dean KT 2013. *Cyber-Security Holism: A System of Solutions for a Distributed Problem*. Coll Quantico VA: Marine Corps Command and Staff.

Dictionary MW 2015. An Encyclopaedia Britannica Company. From <http://www. merriam-webster.hh. com/dictionary/pharmacogenomics> Wikipedia.org.

Fadun OS 2013. Corporate governance and insurance company growth: challenges and opportunities. *International Journal of Academic Research in Economics and Management Sciences*, 2(1): 286.

Imgraben J, Engelbrecht A, Choo KR 2014. Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. *Behaviour and Information Technology,* 33(12): 1347-1360.

Kasemsap K 2017. Internet of Things and security perspectives: Current issues and trends. In: N Jeyanthi, R Thandeeswaran (Eds.): *Security Breaches and Threat Prevention in the Internet of Things*. IGI Global, pp. 19-45. DOI: 10.4018/978-1-5225-2296-6.ch002

Li X, Zhang T 2017. An exploration on artificial intelligence application: From security, privacy and ethic perspective. In: *Cloud Computing and Big Data Analysis (ICCCBDA), 2017 IEEE 2nd International Conference, IEEE*, April, pp. 416-420.

Öðütçü G, Testik ÖM, Chouseinoglou O 2016. Analysis of personal information security behavior and awareness. *Computers and Security*, 56: 83-93.

Patrick, H, Fields Z 2017. A need for cyber security creativity. In: Z Fields (Ed.): *Collective Creativity for Responsible and Sustainable Business Practice*. Hershey, PA: IGI Global, pp. 42-61.

Pawlak P, Wendling C 2013. Trends in cyberspace: Can governments keep up? *Environment Systems and Decisions*, 33(4): 536-543.

Rajra B, Deepa AJ 2015. A survey on network security attacks and prevention mechanism. *Journal of Current Computer Science and Technology*, 5(2). doi.http://dx.doi.org/10.15520%2Flcesto. 2015. vol5.iss02.35

Shafqat N, Masood A 2016. Comparative analysis of various national cyber security strategies. *International Journal of Computer Science and Information Security*, 14(1): 129.

Simpson B, Murphy M 2014. Cyber-privacy or cyber-surveillance? Legal responses to fear in cyberspace. *Journal Information and Communications Technology Law,* 23(3): 189-191.

Walters R 2014. Cyber-attacks on US companies in 2014. *The Heritage Foundation*, 4289: 1-5.

Wu DD, Olson DL 2015. Financial risk management. In: DL Olson, DD Wu (Eds.): *Enterprise Risk Management in Finance.* UK: Palgrave Macmillan, pp. 15-22.

Zureich D, Graebe W 2015. Cybersecurity: The continuing evolution of insurance and ethics *Defense Counsel J,* 82(2): 192-198.

Paper received for publication on August 2016
Paper accepted for publication on December 2016