PUPIL: International Journal of Teaching, Education and Learning
ISSN 2457-0648

Essang Onuntuei, 2018

Volume 2 Issue 2, pp. 81-97

Date of Publication: 21st July 2018

DOI-https://dx.doi.org/10.20319/pijtel.2018.22.8197

This paper can be cited as: ONUNTUEI, E. (2018). Safety, Risk, and Reliability of Cyber Network in Oil and Gas Industry. PUPIL: International Journal of Teaching, Education and Learning, 2(2),81-97.

SAFETY, RISK, AND RELIABILITY OF CYBER NETWORK IN OIL AND GAS INDUSTRY

Essang ONUNTUEI
Humanities Department, Greensprings School, Lagos, Nigeria
Essang@Live.Co.Uk

Abstract

As cyber network cuts across all works of life, several endemic dangers abound. Cyber theft and loss of resources to unauthorised persons has brought a grave concern to the public despite efforts to prevent its occurrence. So, the study considered the link between percentages of systems attacked and insiders' cyber exploits; the impact of early threat detection on prompt response to cyber-attacks, and whether the percentage of systems attacked is a function of threat response duration and cyber welfare package in Nigeria's major oil and gas firms as well. The methods of data analysis used include Pearson product moment correlation, Chi-square, and multiple regression analysis respectively. The results of findings show a link between the percentage of systems attacked and insiders' cyber exploits in Nigeria's major oil and gas firms; early threat detection impacting on prompt response to cyber-attacks, and percentage of systems attacked is a function of threat response duration and cyber welfare package respectively. Also, based on findings, recommendations were made on safety, risk, and reliability of cyber network in Nigeria's oil and gas industry.

Keywords

Cybercrime, Cyber Exploit, Detection, Response, Safety, Threat, Welfare

1. Introduction to the Study

Presently, the world has become a global village where everyone relies on the cyber network for effectiveness and efficiency. Such development has resulted in regional and global benefits. Evidently, adverts, banks, business, jobs, research, teaching, and others have become effective and efficient through the cyber network on global and national scale respectively. Accordingly, there is a "swift growth of ICT taking place all over the world" (Buttar S., 2016). Sadly, while cyber exploits are ongoing, there are reports of it becoming an attractive target for crime, hence, growing concerns for users' safety (Adelola T., Dawson R. & Batmaz F., 2014; Shahid, A. & Sumbul, M. 2017). Many organizations are losing so much data, fund, and resources to unauthorised persons with great depths of breaking through any data, knowledge, programs, strategy, and tools protecting them. For instance, Britain is being targeted by up to 1,000 cyber-attacks every hour. Again, recent cyber-attacks like Anthem Blue Cross and Blue Shield, United Airlines and American Airlines cost average American company $15.4 million per year (Pwc.co.uk, 2015). Such reports bring huge concern over our bank savings, private and public data and since they are linked to cyber, hence a look at 'the state of the art in cyber-attack detection strategies' (Raiyn J., 2014).

Similarly, Nigeria has witnessed hackers break into cyber networks with unhealthy motives. Mr. Adebayo Adelabu- Deputy Governor, Financial Systems Stability of Central Bank of Nigeria said that 2.4% of banking revenue (a sum of 159 billion naira) was lost to cyber fraud within 2000 and the 1st quarter of 2013. He said that while Africa own its place as the region with most online fraud cases, sub-Saharan Africa kept her unenviable rank among regions surveyed as the region with most rife fraud conundrum with 77% (PM News Nigeria, 2015).

Such absorbing worry is worsening by insiders' unabated role to wreck cyber-attacks. Essentially, as many are cyber inclined, their safety remains crucial and efforts to do so yield little or no convincing result; hence, a search for respite continues. Also, reviews on 'current research of IoT, key enabling technologies, major IoT applications in industries, and research trends and challenges' have been made (Xu L., He W. and Li S., 2014). Previous work has listed insiders' role as one of the causes of cyber-attacks yet, no critical look has been made to unravel the 'behind the scene' statements of these hackers. Some say their actions are for fun while culling from it; yet, causing others nightmare. Therefore, Gaines C. & Rashleigh J. (2015) wondered if one is 'taking the right steps when it comes to cybersecurity?' (Gaines C. & Rashleigh J. in https://www.pwc.co.uk).

Inferentially, one may ask: if cyber risks occur frequently in Britain and United States- developed regions, what response do less developed nations like Nigeria have to offer? Can we say Nigeria is in “no respite” situation? Is there any hope for her future cyber networking? Against these backdrops was the study focussed on insiders’ cyber exploits and aim at proffering respite. To substantiate the above claim, the following contributions were made:

- Device tracking technique for staff cyber exploits.
- Prompt Cyber Response program for cyber-attacks in oil and gas firms.
- Design staff improved periodic cyber welfare package for oil and gas firms.

As every staff is asked to ‘Bring-Your-Own-Device’ (BYOD) to work- in other to keep taps with insiders’ activities, and the policy has been adopted by some corporate bodies (Herrera A., Ron M. & Rabadão C., 2018); the approach seems inadequate, ineffective, inefficient and not decisive in nature as control systems are continuously being hacked to date without authorisation; hence the need for a solution.

1.1 Statement of the Problem

We live in a digital era where cyber creates, stores, retrieve, sends and analyses data. For instance, some researchers have focused on the introduction of tablet devices and other computer-related software as new stationery in schools leading to efficiency and viability (Suzuki, T. 2015; Kohsamut, T. & Sucaromana, U. 2017). Nonetheless, such exciting benefits are not without safety issues of endless records of data hacking, endemic theft and so on. Hackers continue to throw sudden sharp, forcible twists or turn into cyber networks leaving most industries’ data integrity in doubt (Buchanan B., 2017).

So, how do we safeguard the system from total collapse? What response do third world countries like Nigeria have to offer amidst cybercrime? Can we say Nigeria’s oil and gas firms are in “no respite” situation? Is there hope for future cyber networking? Can insiders’ cyber deeds be addressed in oil and gas sector? It was against these backdrops that the study was considered: to probe insiders’ cyber-risks exploits; the function of threat response duration and cyber welfare package on the percentage of systems attacked respectively.

1.2 Purpose of the Study

The following objectives were considered in the study:

- To explore the link between systems attacked and insiders’ cyber exploits in Nigeria’s Major oil and gas firms.
- To find out whether early threat detection has a significant impact on prompt response to Cyber-attacks in Nigeria’s major oil and gas firms.

- To examine whether systems attacked in oil and gas firms is a function of threat response Duration and cyber welfare package respectively.
- To explore how to curb insiders' exploits in Nigeria's major oil and gas firms.

1.3 Significance of Study

The study focussed on insiders' cyber-risk deeds in Nigeria's oil and gas firms; hence, its findings may be used by corporate bodies, government and individuals as a claim in strategic policy planning and implementation as well as the basis for further studies.

1.4 Research Questions

To achieve set objectives, the following research questions were formulated:

- What is the link between the percentage of systems attacked and insiders' cyber exploits in Nigeria's major oil and gas firms?
- Does early threat detection have a significant impact on prompt response to cyber-attacks in Nigeria's major oil and gas firms?
- Are systems attacked in Nigeria's major oil and gas firms a function of threat response duration and cyber welfare package as well?
- How can insiders' cyber-attacks in Nigeria's major oil and gas firms be curbed?

1.5 Research Hypotheses

For the purpose of the study, the following hypotheses were considered:

H1: There is no statistical correlation between percentages of systems attacked and Insiders' cyber exploits in Nigeria's major oil and gas firms.

H2: Early threat detection has no significant impact on prompt response to cyber-attacks on Nigeria's major oil and gas firms.

H3: Percentage of systems attacked is not a function of threat response duration and welfare package respectively.

1.6 Scope and Delimitation of the Study

The study was restricted to cyber safety issues in Nigeria's oil and gas industry and their significant impacts on the sector. Most especially, the seemingly insignificant role of insiders' cyber exploits was given great consideration. Also, systems attacked were explored to ascertain whether was a function of threat response duration and cyber welfare package in oil and gas firms and seek to proffer solutions and recommendations as well.

2. Literature Review

A lot has been said about cyber and its related challenges in the past to include its safety, risk, and reliability across the globe. An overview of cyber safety, risk definition, and identifying reasons and challenges were given as well. Also, the highlight of stepping up safety and security, logical and practical solutions to curb the menace was shown (Hollnagel, E. 2018). Be that as it may, while many agree that the cyber benefits outweigh its challenges, others disagree with the claim (PM News Nigeria, 2015).

However, in a debate on reducing cyber risk and vulnerability, one 'will argue that the AU Convention on Cyber Security and Personal Data Protection does not offer adequate basis for mutual help and international alliance amongst African States and that the situation may limit and fragment international alliance and mutual help along sub-regional lines or bilateral bargains' (Orji U., 2015). Some hackers have moved from gambling with servers and operating systems to exploiting computer browsers and email level of users (Chou, T. 2013).

2.1 Historical Development of Oil and Gas in Nigeria

Oil and gas operations first started with the first trading quantity in Oloibiri (Niger Delta) in 1956 by Shell, followed by other multinational oil firms like Gulf oil and Texaco (now Chevron), Elf Petroleum (now Total), Mobil, and Agip, in addition to Shell. Till date, Nigeria ranks Africa's second largest and eleventh world's largest oil producer as well (www.nnpcgroup.com/NNPCBusiness/upstreamventures/oilproduction.aspx). According, to a BBC Newshour Extra report of January 08, 2016 at 9:08 GMT, oil represents 90% of the country's foreign exchange earnings and 80% for the local dependence of her budget. With current decline in the price of oil in the global market, many states in Nigeria are unable to pay workers' salaries for several months, hence, a cry on the 'end of oil' predicts sharp fall in financial revenue and huge security concerns (BBC Newshour Extra, 2016).

2.2 Background of Cyber Safety, Risk, and Reliability

Both theoretical and investigative approach were used to reveal sociological and technological factors affecting Nigeria's cybercrime and articulate its relevant conditions and threats (Olayemi O., 2014). Also, five research challenges facing the domain were outlined with possible measures to be taken were mentioned (Cherdantseva Y., Burnap P., Blyth A. Jones K., Soulsby H., & Stoddart K., 2016). Again, a comprehensive framework for risk assessment of cyber damages in the absence of any and built a taxonomy of possible cyber catastrophe scenarios was established to review 'the state of the art in cybersecurity risk assessment of Supervisory Control and Data Acquisition (SCADA) systems' (Cherdantseva Y., Burnap P. Blyth A. Eden P., Jones K., Soulsby H. & Stoddart K. 2016). More so, 'cyber risk insurance underwriting to model risk control beyond Value-at-Risk (VaR), pre-empt and prevent global cyber-insurance crisis was set forth' (Malhotra, Y. 2017). 'Reports of a novel integrated approach for safety analysis and security analysis of systems' were made. (Pereira

D., Hirata C., Pagliares R., & Nadjm-Tehrani S., 2017). Their findings showed ‘that their approach allowed security and safety teams to perform a more efficient analysis.

2.3 Impact of Cyber Safety on Energy Sector

The Nigerian Voice (2015) report findings of a research team on Nigeria and cyber-related fraud and said Nigerian scams cost the British economy £150 million a year, while some countries lose at least $36 million a year to Nigerian scams, and some other countries send at least $3 million a month to Nigeria of which at least 80% is cyber fraud-related. The scholar says the cyber cost to society goes beyond just losing money as some victims have attempted suicide while others watch their businesses go bankrupt. Oil and gas facilities are a major target for extremists to cause economic damage and project their influence as well (Helms J., Salazar B., Scheibel P., Engels M., & Reiger C., 2017). They believed that ‘cyberattack can have highly negative impacts on energy delivery systems (EDS).’

Findings reveal that Less Developed Countries feel most cyber risk impacts. But other studies reject such claim adding that the economic and literacy level of third world countries do significantly hinder cyber exploits. Nevertheless, other sets of scholars were neither for nor against both dispositions, citing that each scenario was significantly unique in its presentation. Consequently, these divergent views led the researcher to look inward- Nigeria and make his own contribution to the body of knowledge. A more growing concern lies in the fact that no research considered whether the impact of cyber risk and vulnerability is same for all major oil and gas firms in the country or otherwise, hence the scholar was led to explore cyber-related crime in oil and gas and make statements of fact.

2.4 Reducing Cyber-Related Challenges in Energy Sector

Cyber in oil and gas industry in Nigeria is useful to International oil firms and National oil firms within. However, scholars claim a lot of challenges hinder its benefits. As a way forward, a 3D threat model for the IoT was proposed along with the discussion on nine security challenges and several ways to mitigate risks as well (Bhattarai S. & Wang Y. 2018). Also, ways to detect, improve cyber network high availability and prevent cyber-threats was disclosed (Stephan R., Stereshkov V., 2018). In a related development, Herrera A., Ron M. & Rabadão C., (2018) mentioned best ways to ensure information security. They include using a multi-layered security, updating and upgrading against new hacking techniques and technologies, encrypting all data, keeping an eye on staff’s habits in handling data and securing data in Bring-Your-Own-Device (BYODs) as well.

2.5 Expert Opinions and Current Debate on Cyber Safety

While most experts say we live in an interconnected world where the role of cyber need not be overemphasized, others argue that cyber-hacking is going to increase as the internet of things become a reality (Chen, E. 2017). In a fight against cybercrime, the U.S. passed a concurrent resolution to protect firms that relate cyber threat data with the government. Also, under consideration by the legislature are the Protecting Cyber networks Acts and the National Cyber Security Protection Advancement Act of 2015. Nevertheless, the difficulty in securing the cyber network is linked to attackers' ability to operate from any location, connections between cyberspace and physical systems, and complex nature of the cyber network, thus making it so difficult for tracking (Trautman, L. 2015).

The current debate on cyber safety has centered on keeping businesses and people secure from cyber-attacks while shielding their privacy (Braun T., Fung B., Igbal F. & Shah B. 2018). While the scholar says U.S. government aims at protecting firms that relate cyber threat data with them, contrary opinion argues that no one trusts anybody while feeling like giving the government too much power to breach privacy. Again, others believed that government lacks credibility and competence in handling the task when compared to private institutions. As alternative measures, cyber education enhancement and encouragement of the private sector to lead in cyber safety seem the way forward. From the foregoing, it was clear that if the contextual and situational issues play a significant role in sharing cyberattacks, then the expert of the team remains important in the fight against insiders' cyber-risk deeds. In the light of these concerns, the researcher posited that the only reason for continued cyber theft was due to failed methodologies in the past. Therefore, it was the researcher's goal to focus on the insiders' deeds, an often forgotten component of research studies on cyber-attack, to gain a clear view on their operations, and how best to curb such attacks. He believed a way forward shall be attained in the near future citing his proposed methodology as one since no previous consideration had ever been given it a taught.

3. Research Design

The research design considered a pre-test, post-test quasi-experimental non-randomized experimental group, and a control group. The method provided a strong benefit for data collection and compared scores from both groups while giving a summary of the strategy adapted to cyber safety. Respondents for the study came from six (6) oil and gas firms with similar ability and makeup to form the control and experimental group respectively. Each group had a team of three oil and gas firms. The control group comprised of NNPC, Shell, and Total while the experimental group was made up of Chevron, Exxon Mobil, and Oando respectively as shown in Figure 1 below.

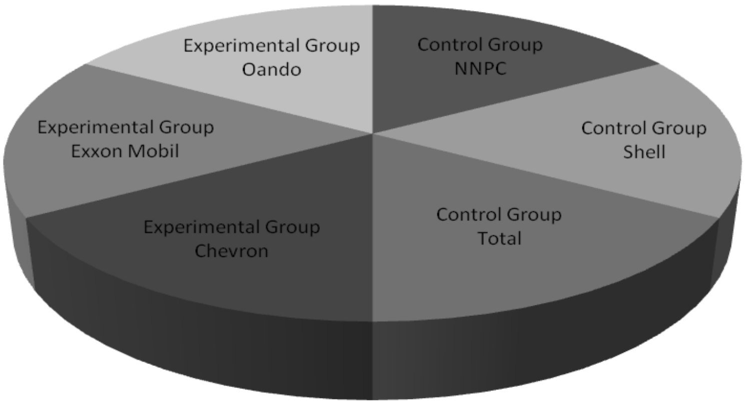

Figure 1: *Showing the Distribution of Respective Groups*
Source: Survey

Firstly, the aim of the study was introduced to respondents in each group before conducting a pre-test survey to rate their methods in controlling insiders' cyber deeds and attacks given similar conditions. While the control group secured cyber network using normal routine (encryption and firewall), the experimental group adopted a different approach. In addition to encrypting and using firewalls, the experimental group set up a team of experts to track staff's cyber exploits, adopt emergency cyber-response method to detection of an impending cyber-attack and drew strategic plan for staff improved periodic welfare package.

The next step was to collect, organize, and analyze data from respondents in both groups. The post-test was conducted afterward to assess and give a summary of the study. Respective scores were compared for a conclusion on a better approach to curb insiders' cyber-attacks and deeds. Again, the method revealed whether cyber tracking technique, Prompt Cyber Response Program for attacks (PCRP); and designing staff improved periodic welfare package in oil and gas firms (as adopted by experimental group) had an impact on staff cyber exploits respectively.

An explanation of experimental group's approach has it that all respondents in each firm were shared with a group of ten with one team expert to supervise their cyber exploits. The supervision of team members' cyber deeds was in addition to traditional network security of firms. While each team member engaged in cyber deeds, respective team supervisors strictly monitor their exploits using their own systems. A summary of design for both groups is shown in Table 1 below:

Table 1: *Showing a summary of design for both groups*

Control Group (NNPC, Shell and Total)	Experimental Group (Chevron, Exxon Mobil and Oando)
• Control room staff served as the only cyber link monitor.	• Minimum of ten computers are linked to each expert's system serving as team supervisor. This is along with the control room staff that is the head of experts' team.
• WEP authentication	• Team expert closely monitored and observed team members' cyber deeds while they are at still at work.
• Encryption of communication between devices within a network.	• At close of work, team expert analyzed team members' online-cyber-deeds using his assigned computer with a program that detects cyber threats.
• Install and maintain configuration to protect data.	• Team expert study and appraise each team member's cyber deeds using their assigned system while offline.
• Regularly update anti-virus.	• Team experts to promptly flag up any form of impending cyber threat as observed.
• Maintain a policy that addresses information security for all respondents.	• Encourage respondents to flag up any form of impending cyber threat noticed.
• No risk management team for prompt response upon detection.	• Risk management team to promptly respond upon detection.
• No special welfare package for staff on cyber safety.	• Periodic review of staff inducement for having a risk free computer after careful analysis.
	• Staff inducement to participants for flagging perceived threats without delay or denial.
	• Discourage use of a personal system, external hard drive.
	• Special welfare package for all committed and dedicated staff member.

Source: Survey

3.1 Sample and Sampling Technique

A purposive sampling technique was employed in selecting both sample groups based on convenience with respect to operation, sector, facility and equipment and location as well. These involved researcher's opinion on what should be sampled or not, focus on certain specified characteristics and ensure that only samples with required purpose and attributes were selected. Therefore, sampling without replacement, where each sample was chosen just once and not replaced before drawing up the next, was adopted. A total of three hundred (300) respondents from both groups were selected as sample for the study (i.e. 150 from each group). As the target population was so large and the geographical area was rather wide to cover considering cost, and other constraints, it became very important to curl out a sample for the study as may be seen in the group bar chart in Figure 2 below. From the bar graph, a 100% makeup of each sample group was determined for respective firms.

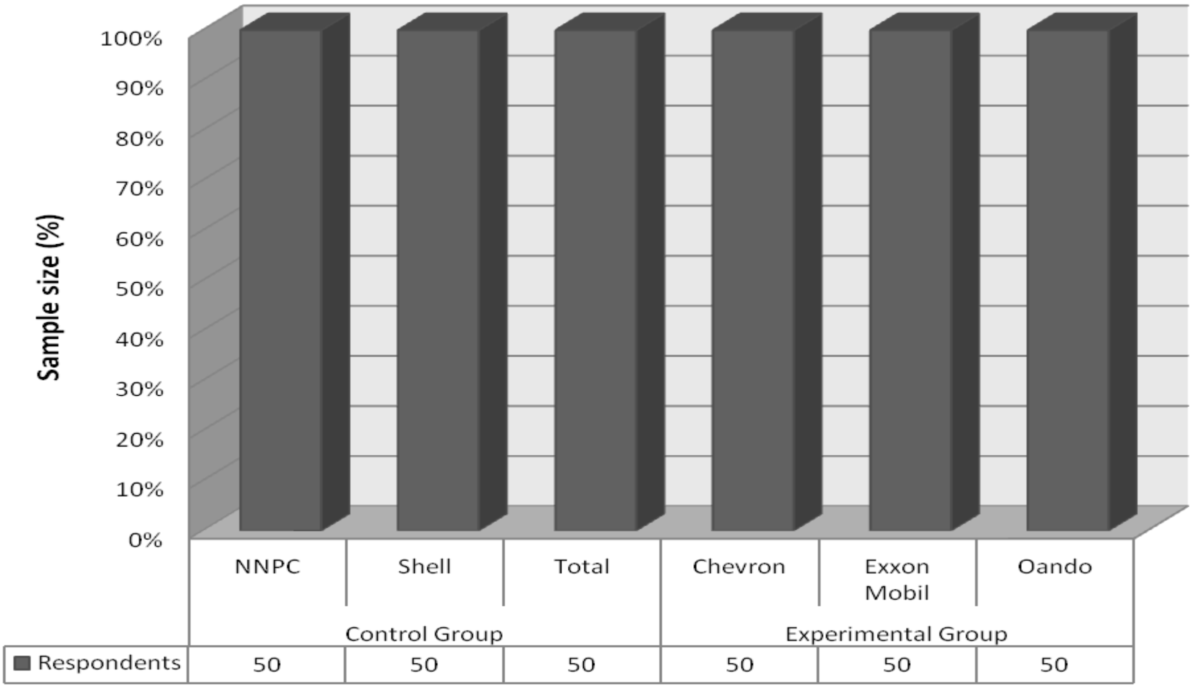

Figure 2: *Showing Sample size Distribution*
Source: Survey

3.2 Method of Data Analysis and Procedure

The method of data analysis was Pearson moment correlation. The method used determined the link between all Nigeria's major oil and gas firms and insiders' cyber-attacks. In other words, the method used established if all Nigeria's major energy firms do suffer insiders' cyber-attacks. Again, the method tested the impact of Insiders' cyber deeds on Nigeria's major oil and gas firms. In other words, the method was used to establish whether insiders' cyber-attack deeds have an effect on Nigeria's major oil and gas firms.

The pre-test and post-test survey conducted for both groups were presented graphically in Figure 3 and Figure 4 below. A comparison between both surveys showed the level of cyber-attacks on major energy firms and respective impacts of tracking techniques on cyber threats. More so, the effect of prompt response program on detection of impending cyber-attacks proved significant on the level of systems attack by insiders' cyber exploits. By introducing cyber threat welfare package for staff, the level of systems attacks reduced in the experimental group. Furthermore, Figure 5 and 6 represent a change in Insider's cyber Deeds and Systems attacked.

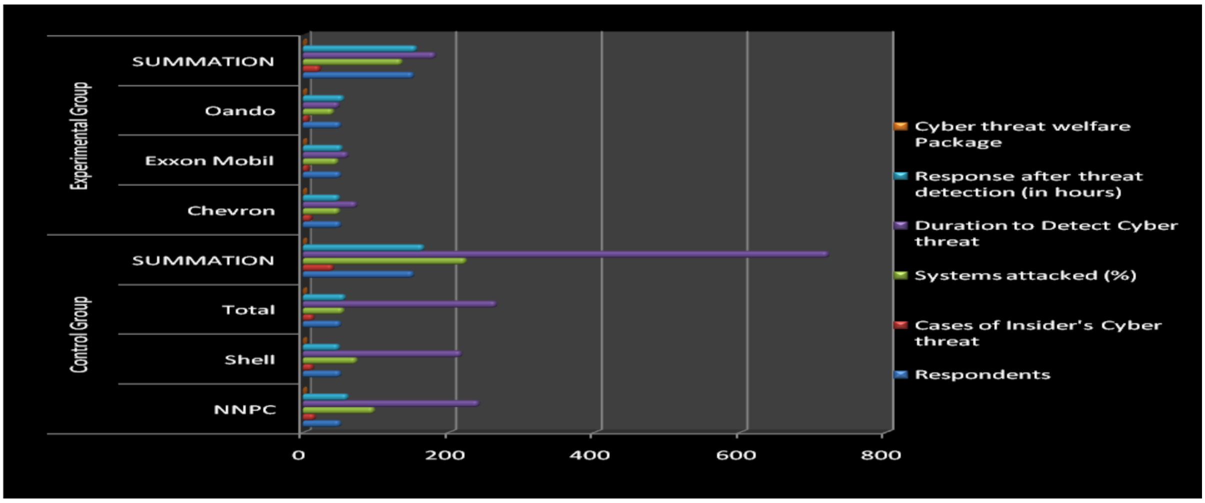

Figure 3: *Showing Pre-Test Survey on Insiders' cyber-attack control*
Source: Survey

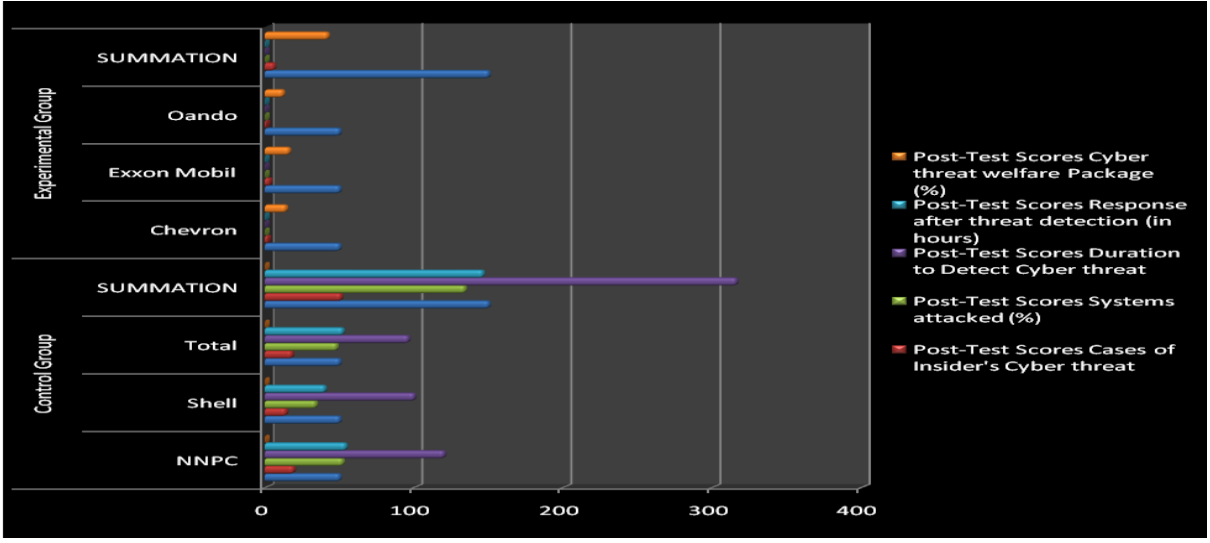

Figure 4: *Showing Post-Test Survey on Insiders' cyber-attack control*
Source: Survey

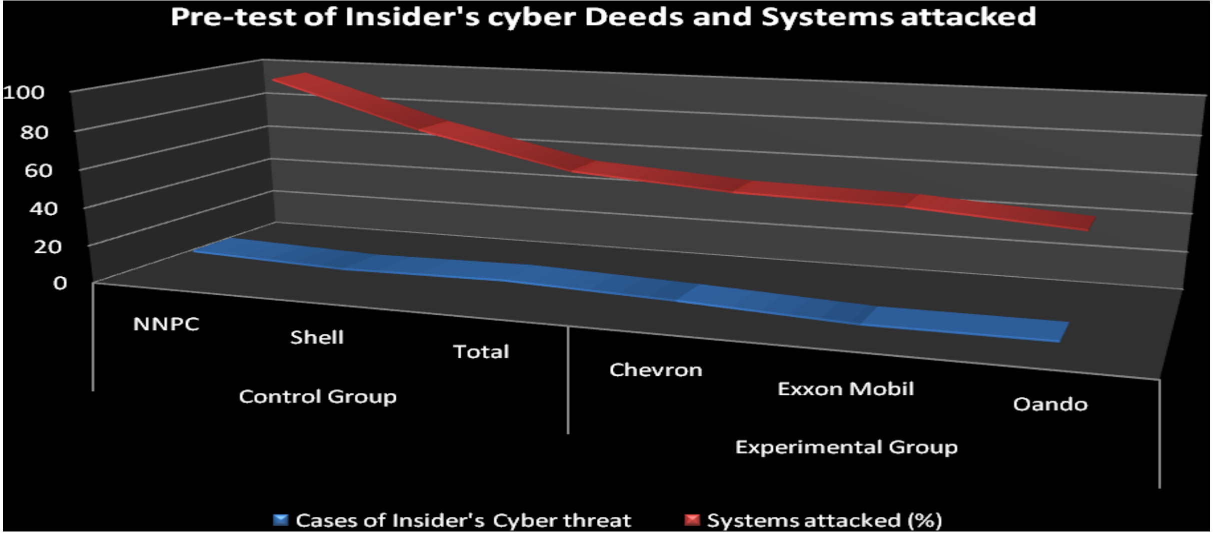

Figure 5: *Showing Pre-test of Insider's cyber threats and Systems attacked*
Source: Survey

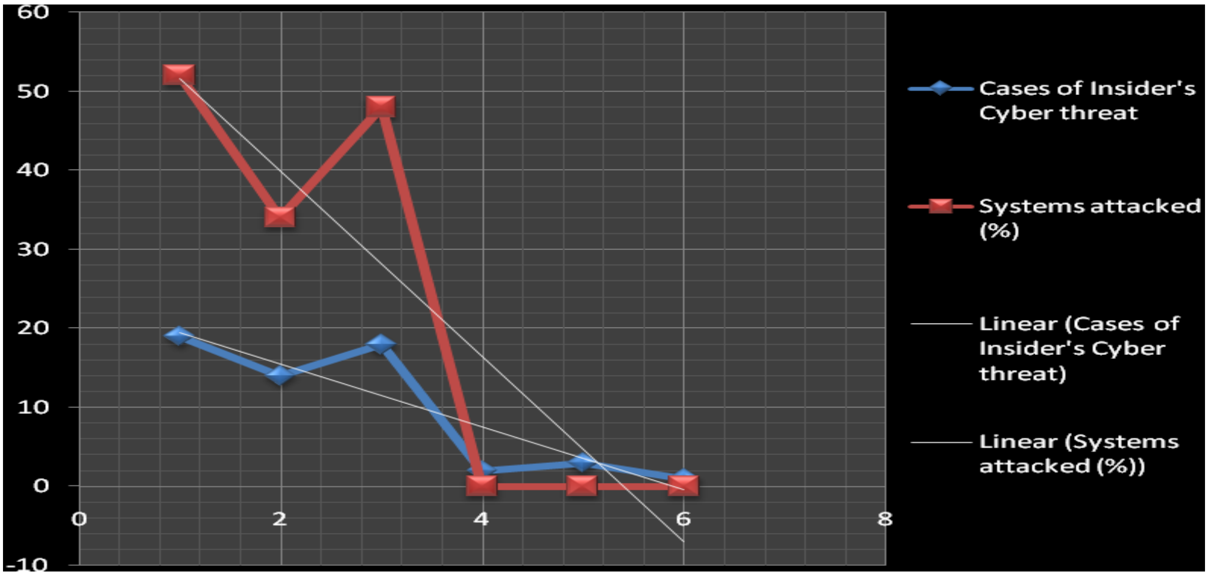

Figure 6: *Post-Test Scattergram of Insider's cyber threat and systems attacked*

In the pre-test survey as represented in Figure 5, cases of insiders' cyber deeds and systems attacked level was high especially for the control group. On the other hand, the post-test survey as represented in Figure 6, revealed that the experimental group recorded low scores in both cases of insider's cyber deeds and systems attacked respectively. Same was not the case of the control group which was still high in their records.

4. Summaries of Major Findings

Statistically speaking, the following served as major findings of the study:

- All Nigeria's major oil and gas firms do suffer insiders' cyber-attack.
- Insiders' cyber-attacks do impact on Nigeria's major oil and gas firms.
- Statistically, a correlation exists between percentages of systems attacked and Insider's cyber exploits in Nigeria's major oil and gas firms.
- Tracking technique for cyber activities of Nigeria's oil and gas staff impact on insiders' cyber-attacks.
- Prompt cyber response program in oil and gas firms is an effective and efficient means of curbing cyber-attacks.
- Early threat detection and improved cyber welfare package for Nigeria's oil and gas staff has a significant impact on systems attacked.
- A multiple regression of threat detection response and cyber threat welfare Package explained the percentages of systems attacked.

4.1 Interpretation of Findings

The study established statistically that all Nigeria's major oil and gas firms do suffer insiders' cyber-attack. The result showed that loss of information and systems attacked were a function of insiders' cyber-attack exploits. About 99.3% of the variance in Insiders' cyber exploits has been explained by percentage of systems attacked in Nigeria's major oil and gas firms. The result goes to show that where there were frequent insiders' cyber deeds; increasing record of systems damage was noticeable.

Again, the result showed that early threat detection has a significant impact on prompt response to cyber-attacks in Nigeria's major oil and gas firms. The team of experts played a significant role in tracking staff cyber exploits which in turn reduced cyber risks. At 98.5% of the variance in response after threat detection, an explanation on the number of duration of threat detection was made. The adoption of prompt cyber emergency response upon detection of impending attacks reduced cyber losses.

Also, a 72% threat detection response and cyber threat welfare Package explained the rate of systems attacked in oil and gas industry in Nigeria as well. Staff inducements significantly deter insiders' deal in cybercrime by 72% based on the findings of the study as well.

4.2 Discussion of Findings and Research Limitations

As shown in the analysis of hypothesis one, a total of 134% of systems attacked from 57 cases of insiders' cyber threat was recorded in sampled oil and gas firms in Nigeria, representing x and y variables respectively. $\Sigma x2 = 6,164$; $\Sigma y2 = 895$; $x = 22.3$; $y = 9.5$; correlation (r) = +0.9964 indicating a very high positive relationship correlation. The findings of the study showed that all Nigeria's oil and gas firms do experience cases of insiders' cyber-attack deeds. However, their level of occurrence differed between control and experimental group respectively due to certain factors worthy of mention. They include tracking techniques for cyber activities; prompt cyber response program; designing improved cyber welfare package for Nigeria's oil and gas staff respectively.

Similarly, a 98.5% significant impact of early threat detection was observed on prompt response to cyber-attacks in Nigeria's major oil and gas firms. The study revealed a +0.9925 high positive correlation between early threat detection response to cyber-attacks in oil and gas firms. Finally, a multiple regression of threat detection response and cyber threat welfare Package explained the percentages of systems attacked in oil and gas industry. Both variables (threat detection response and cyber threat welfare Package) explained the rate of systems attacked in oil and gas industry at about 72% respectively. The formula for the equation was given as thus: $y = -0.38 + 0.72(x1) + 0.72(x2)$.

Major limitations of the study include funding, the time frame for the study and the non-corporative attitude of some responders. These limitations impact significantly on sample size obtained for the study.

4.3 Implications of the Study

In reference to the study, the following implications were deduced:

- That all Nigeria’s major oil and gas firms do suffer insiders’ cyber-attack.
- Insiders’ cyber-attacks do impact on Nigeria’s major oil and gas firms.
- A link exists between systems attacked and Insiders' cyber exploits in Nigeria’s major oil and gas firms.
- Early threat detection does significantly impact on prompt response to cyber-attacks in Nigeria’s major oil and gas firms.
- Systems attack is a function of response to threat and cyber welfare package respectively.
- Solid cyber-risk measures in oil and gas firms serve as the basis for establishing an Excellent-secure-cyber network beyond the sector and nation as a whole.

5. Recommendations

Based on the discussion and research findings of the study, the following recommendations were made:

- All Nigeria’s major oil and gas firms should adequately monitor insiders’ cyber-attack deeds with utmost priority.
- Government and management of corporate organizations should be deeply involved in insiders’ cyber-attack deeds in Nigeria’s major oil and gas firms.
- Adequate and regular training on tracking the dynamic nature of insiders’ cyber-attack exploits in oil and gas sector should be given priority.
- Tracking the dynamic state of insiders’ cyber-risk deeds should be regardless of roles played by system control team and Information Technology team in oil and gas sectors.
- Improved security measures should be put in place to track the changing state of insiders’ cyber-attack deeds in oil and gas sector.
- Prompt cyber response program for in energy sector is strongly recommended in curbing insider’s cyber-attacks exploits.
- Designing improved cyber welfare package for Nigeria’s oil and gas staff is recommended as an effective, efficient and useful means to curb cyber risks.

5.1 Scope of Future Research

An extensive research is needed to explore the effectiveness of dealing with cyber safety, risk, and reliability from insiders’ cyber-attacks’ point of view in oil and gas firms. Also, the need to promote corporate partnership among Nigeria’s major oil and gas players in exploring cross-sectional time series analysis of insiders’ cyber deed is suggested. Again, the further comparative study of significant impacts of cyber laws among world’s regions should be considered as well. The aim of these studies shall be to lay rest debates on curbing insiders' cyber-attack deeds

References

Adelola, T., Dawson R. and Batmaz, F. (2014). 'Privacy and data protection in E-commerce: The effectiveness of a government regulation approach in developing nations, using Nigeria as a case,' The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014), London, pp. 234-239. https://doi.org/10.1109/ICITST.2014.7038812

BBC Newshour Extra (2016) 'The end of oil and its implications,' Radio program on January 08, 2016 at 9:06 GMT.

Bhattarai, S. & Wang, Y. (2018) 'End-to-End Trust and Security for Internet of Things Applications' Computer (Vol. 51, Issue: 4, April 2018). https://doi.org/10.1109/MC.2018.2141038

Braun T., Fung B., Igbal F. & Shah B. (2018) 'Security and privacy challenges in smart cities.' Sustainable Cities and Society. Vol. 39, Pp 499-507. DOI: https://doi.org/10.1016/j.scs.2018.02.039

Buchanan, B. (2017) The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190665012.003.0009

Buttar, S. (2016). 'ICT in Higher Education' PEOPLE: International Journal of Social Sciences Vol. 2 Issue 1, pp. 1686-1696. - http://dx.doi.org/10.20319/pijss.2016.s21.16861696

Chen, E. (2017) The Internet of Things: Opportunities, Issues, and Challenges In: The Internet of Things in the Modern Business Environment. Pp21. https://doi.org/10.4018/978-1-5225-2104-4.ch009

Cherdantseva Y., Burnap P., Blyth A. Jones K., Soulsby H., & Stoddart K., (2016) 'A review of cyber security risk assessment methods for SCADA systems' Computers & Society Volume 56, February 2016, Pages 1-27. https://doi.org/10.1016/j.cose.2015.09.009

Chou, T. (2013). 'Security threats on cloud computing vulnerabilities' International Journal of Computer Science & Information Technology (IJCSIT) Vol 5, No 3, June 2013 www.academia.edu/download/39196617/5313ijcsit06.pdf

Fishler, M. in AZ Big Media, (2015) Cyber security causes concerns about privacy; Dated: 2nd January, 2015. https://azbigmedia.com/publications/arizona-bankers-association-2015-2/ https://azbigmedia.com/publications/arizona-bankers-association-2015-2/

Gaines C. & Rashleigh J. (2015). Are you taking the right steps when it comes to cyber security? Retrieved from: https://www.pwc.co.uk/issues/cyber-security-data-privacy/are-you-taking-the-right-steps-when-it-comes-to-cyber-security.html

Helms J., Salazar B., Scheibel P., Engels M., & Reiger C., (2017). Safe Active Scanning for Energy Delivery Systems Final Report. Lawrence Livermore National Security https://doi.org/10.2172/1409972

Herrera A., Ron M. & Rabadão C. (2018) 'National cyber-security policies oriented to BYOD (bring your own device): Systematic review' Information Systems and Technologies (CISTI), 2017 12th Iberian Conference. DOI: https://doi.org/10.23919/CISTI.2017.7975953

Hollnagel, E. (2018) Safety I and safety II: the past and future of safety management. London: CRC Press

Kohsamut, T. & Sucaromana, U. (2017) 'Using Blog to Enhance English Writing Skill Among High School Students in Thailand' PEOPLE: International Journal of Social Sciences. Volume 3 Issue 2, pp.1337-1348. DOI- https://doi.org/10.20319/pijss.2017.32.13371348

Malhotra, Y. (2017) Advancing Cyber Risk Insurance Underwriting Model Risk Management beyond VaR to Pre-Empt and Prevent the Forthcoming Global Cyber Insurance Crisis (December 7, 2017). https://doi.org/10.2139/ssrn.3081492

Nigerian National Petroleum Corporation (2016). Oil Production. Retrieved from: www.nnpcgroup.com/NNPCBusiness/upstreamventures/oilproduction.aspx

Olayemi, O. (2014) A socio-technological analysis of cybercrime and cyber security in Nigeria Vol. 6(3), pp. 116-125, Academic Journals. ISSN 2006- 988x © 2014 https://doi.org/10.5897/IJSA2013.0510

Orji U. (2015) 'Multilateral legal responses to cyber security in Africa: Any hope for effective international cooperation?' Cyber Conflict: Architectures in Cyberspace (CyCon), 2015 7th International Conference https://doi.org/10.1109/CYCON.2015.7158472

Pereira D., Hirata C., Pagliares R., Nadjm-Tehrani S. (2017) 'Towards Combined Safety and Security Constraints Analysis' In: Tonetta S., Schoitsch E., Bitsch F. (eds) Computer Safety, Reliability, and Security. SAFECOMP 2017. Computer Science, vol 10489. Springer, Cham Doi: https://doi.org/10.1007/978-3-319-66284-8_7

PM News Nigeria (2015) Cyber Crime in Nigeria. Dated: 6 June, 2018 http://www.pmnewsnigeria.com/2015/06/24/cyber-crime-in-nigeria/

Pwc.co.uk (2015) Information Security Breaches Survey. Dated: 11 August 2015 Retrieved from http://www.pwc.co.uk/audit-assurance/publications/2015-information-security-breaches-survey.jhtml

Raiyn, J. (2014) 'A survey of Cyber Attack Detection Strategies' International Journal of Security and Its Applications Vol.8, No.1 (2014), pp.247-256 https://doi.org/10.14257/ijsia.2014.8.1.23

Shahid, A. & Sumbul, M. (2017). 'Social Evils In Media: Challenges And Solutions In 21st Century.' People: International Journal Of Social Sciences, 3(3), 854-875. DOI-https://doi.org/10.20319/pijss.2017.33.854875

Stephan R., Stereshkov V., (2018) Systems and methods for detecting and preventing cyber-threats - US Patent App. 15/628,917, 2018 - Google Patents. https://patents.google.com/patent/US20180109558A1/en

Suzuki, T. (2015) 'Practice of tablet device classes in Keio Yochisha primary school - ICT Education from primary school first grade' http://grdspublishing.org/PEOPLE/people.html

The Nigerian Voice (2015).'Cyber Crime; the Greatest Challenge of the Nigerian Youths!!!' Dated: 10/14/2015. Retrieved from: https://www.thenigerianvoice.com/news/193648/cyber-crime-the-greatest-challenge-of-the-nigerian-youths.html

Trautman, L. (2015) 'Cybersecurity: What about U.S. Policy?' U. Ill. JL Tech. & Pol'y 341. https://heinonline.org/HOL/LandingPage?handle=hein.journals/jltp2015&div=15&id=&page=

Xu L., He W. and Li S. (2014). 'Internet of Things in Industries: A Survey' IEEE Transactions on Industrial Informatics (Vol.10, Issue: 4, Nov. 2014) Page(s): 2233 – 2243 https://doi.org/10.1109/TII.2014.2300753