International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 3, pp: 335-343 www.ijaem.net ISSN: 2395-5252

Synopsis of Cyber-attacks Incidents and Impacts on Oil and Gas Critical Infrastructures: A Nigerian Perspective

Achunike, Victor U., Egbuna, Fidelis C.
Adjunct Lecturer, Dept. of Computer Science, Institut Bilingue Libre Du Togo, Lome
Adjunct Senior Lecturer, Dept. of Computer Science, Institut Bilingue Libre Du Togo, Lome
Corresponding author: Achunike

Date of Submission: 25-07-2020 Date of Acceptance: 05-08-2020

ABSTRACT — Nearly every sector depends on Information Technology, IT and the internet for its operations. The Oil and Gas sector is inclusive, because digitally connected oil and gas operations such as— exploration, production, processing, storage, and transportation of petroleum liquids and natural gas, help to improve production. These days, however, technology dependence has led to greater vulnerabilities for attackers to exploit. Although, in Nigeria, from cybersecurity perspectives, the popularly reported breaches seem limited to hacking of Facebook accounts and other social media applications. The truth is that, no nation can downplay the threat of a looming crippling attack on her critical sectors facilities (like Energy). Cyber-attacks can take the form of — cyber war, cyber-terrorism and cyber-crime. With the oil and gas sector fueling every aspect of our daily life, the protection of its critical infrastructure is crucial. Starting with some fundamentals to online security, this paper attempts to reveal some atrocious cybersecurity incidents that the global petroleum industry face and their impacts. The research enumerates some roles that IT, and operational technology (OT) play as critical oil and gas infrastructures. Furthermore, the study called for a dynamic technological integration, deployment and collaboration as essential elements in achieving robust secure processes for steady oil and gas production and profitability.

Keywords—Oil and Gas, information technology, operational technology, cyber incidents, cyber-attacks, critical infrastructure, cybersecurity.

I. INTRODUCTION

The ever increasing energy demand in the world has led to the development of various energy sources. In recent years, there have been escalations in the number of oil and gas companies and offshore installations. There are around 600 oil fields, producing from around 5,000 wells in Nigeria's Niger Delta region. It is an area criss-crossed by approximately 10,000kilometres of pipelines[2]. This production growth comes with accompanying risks and challenges in this industry.

Beyond protecting military information systems, the energy sector is also an area of considerable concern. In Nigeria, the predominant attacks on Oil and gas facilities in different parts of the nation have been physical, as Ejoh E. and Okafor P., (2017) stated [16]. They made reference to the recurrent issues of pipeline vandalism that translated to financial losses running into several billions of dollars. Lowest official data for the quantity of oil spilled put a daily average loss at 93.9 barrels per day, and 712 barrels per day as the worst-case figure [2]. These domestic security threats that included gate blockade, non-violent seizure or occupation of oil facilities, abduction, attacks on oil sites and installations (e.g. wells, pipelines, flow-stations), were defended via the use of electric perimeter fences; highly visible armed guards; and negotiated settlements using company's community liaison officers. According to Africa Oil and Gas Report, the year 2016 saw the highest number of attacks in Nigerian waters since 2008. This was primarily driven by financially motivated kidnapping-for-ransom groups based in Bayelsa and Rivers states of the federation [3].

II. THEORETICAL BACKGROUND

Oil is a very popular commodity due to its high consumption levels. It is the most widely traded commodity, both physically and financially around the world, and in line with the International Energy Agency [30] close to 90 million barrels of oils are utilized globally every day. Current electricity demand in Nigeria is estimated to be between 8,000 - 10,000MW (Megawatts), while available capacity on the national grid averages around 3,500 MW [21]. For this reason, a significant part of energy demand is met by onsite generating-plants which are primarily fueled by petrol and diesel— both products of oil and gas exploration and fractional distillation processes.

Petro-business in Nigeria, especially the upstream or exploration/production sector is currently

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 3, pp: 335-343 www.ijaem.net ISSN: 2395-5252

dominated by the big 'transnational oil companies' (TNOCs), such as Shell, ExxonMobil, Chevron, Texaco, Agip and Elf [29]. They operate joint venture production arrangements with the Nigerian government represented by the Nigerian National Petroleum Corporation, NNPC.

The study is significantly informative and intended to create the much needed awareness of the perils of lacking robust cybersecurity framework; and to add to the existing body of knowledge on matters thereto. These occurrences and recommendations, the researcher hopes that the stakeholders in the industry could review, learn, and adopt, in order to forestall future events and improve overall service delivery.

III. SECURITY IN THE CYBERSPACE

a. Definition of Cyber-attack and Cybersecurity

The word 'cyber' relates to computers and electronic communication networks, especially the Internet [32]. Cyberspace is an interdependent network of critical and non-critical national information infrastructures, through the use of information and communication technologies. It constitutes an arena for a countless number of computing devices that make-up the Internet. Cyberspace makes universal connectivity possible and eases free flow of information, services and ideas [8][31][33].

Cybersecurity architecture is an integral part of the enterprise design that describes the structure and behaviour for an enterprise's security processes, cybersecurity systems, personnel, and subordinate organizations, showing their alliance with the organization's mission and strategic plans. The valuation of security risks begins with the identification of the threats and vulnerabilities, the critical assets, and their impacts.

b. Motivations For Cyber-attacks

Indeed, geo-political tensions, a military incursion or even an ill-judged tweet could trigger a cyber attack on critical national infrastructure. Stuxnet, for instance, was dissected and diagnosed as a pioneering and politically motivated cyber attack. Unfortunately, it successfully infiltrated a high-security, government-run critical infrastructure and destroyed its physical property with computer code [37].

In a Television programme aired on NTA International [14], a security expert and former chief security officer to the Minister of Power and Steel; and to Rivers State governor and currently a private and public consultant, Dr. Dodeye Arikpo named Costa Rica, Malaysia, Malta, Poland, South Africa, Tunisia, Vietnam, Gambia, Liberia, etc., as nations once attacked by North Korea. Countries or organizations could be attacked for the following reasons:

1st — Political or economic gains,
2nd — To obtain critical intelligence and classified data
3rd —To have competitive edge over perceived enemies
4th — And out of sheer malice

He further clarified that, cyber-attacks cannot be prevented, but can be mitigated via well-built cyber walls. Some years ago, the Nigeria's national cybersecurity strategy policy document listed sources of cyber threats to include: organized criminal syndicates, corporate insiders, terrorists and extremist group, among others [8].

c. Forms and Agents of Cyber threats

G. K. Saini, et al., (2019) cited the works of Kumar et al., (2016) which classified the forms of cyber threats as—cyber war, cyber-terrorism and cyber-crime [23]. Firstly, cyber war occurs when one country aims to destroy the networks and computing devices of another. For example, Denial of Service, DoS attacks and viruses. Secondly, cyber-terrorism occurs when terrorist organizations organize activities using cyber means that cause or spread terror. Lastly, cyber-crime is motivated by data theft, monetary gain or wicked-hacking, for example, debit/credit card data, crashing website. Additionally, the authors identified three categories of attacks as:

- Network attacks (Intrusions, Web defacement, Denial-of-Service, DoS attacks)
- Network abuse (Phishing, Forgery, SPAM) and
- Malicious codes (Viruses, Worms, Trojan horse, Spyware, Key loggers, BOTs).

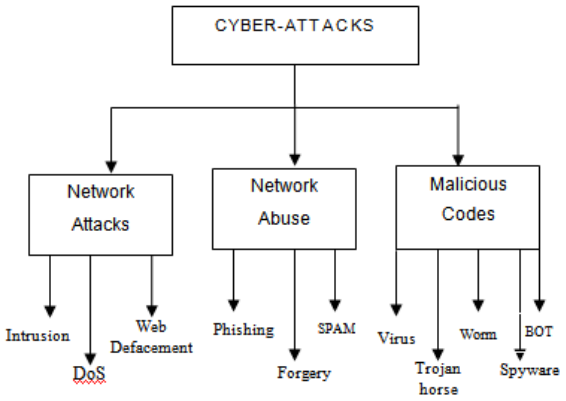

Figure 1: Categories of Cyber-attacks

Source: Developed by writers, based on K.S. Saini, et al (2019)

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 3, pp: 335-343 www.ijaem.net ISSN: 2395-5252

There exist a number of threat agents in the cyber ecosystem. In security parlance, a threat agent is an attack source combining motivation and capability. The Spain's 2019 National Cybersecurity Strategy document [33] describes cyber threats as malicious disruptions or manipulations that affect technological elements. Providing security in information networks and systems requires improving prevention, detection and response measures, and encouraging security. In general, threat agents can be categorised from benign to critical. Table 1 is a breakdown of common threat agent categories and their typical vectors.

TABLE I. THREAT AGENTS AND THEIR VECTORS

THREAT LEVEL	THREAT AGENT	THREAT VECTOR
CRITICAL	Nation state	Espionage, theft, sabotage, product alteration
	Competitor	Espionage, theft, product alteration
	Organised crime	Espionage, fraud, theft
	Terrorist	Sabotage, violence
HIGH	Activist/hacktivist	Espionage, data theft, sabotage
	Disgruntled employee	(All of the below)
	Reckless, untrained or distracted employees	Accidental breach or misuse of data
MEDIUM	Thief	Physical theft, espionage, fraud
	Irrational individual	Physical theft or sabotage
	Vendor or partner	Accidental leak, but also intentional fraud or theft
LOW	Outward sympathiser	Deliberate data leak or misuse of data

Source: (A.Wong, 2016, p48)

IV. OIL AND GAS KEY INFRASTRUCTURES

In terms of security, it is important to consider what, who and how is involved. That is, what devices to protect, who is authorized to apply these measures and how the devices should be protected?

4.1 What are Critical Infrastructures?

Critical infrastructure, CI as depicted by the US Department of Homeland Security in a paper titled: What Is Critical Infrastructure? Are the assets, systems, and networks, whether physical or virtual, so vital that their incapacitation or destruction would have a debilitating effect on national economic security or safety [40]. CI includes any element of a system that is required to maintain functionality and physical security. Computer communication has evolved into CIs. Widely accepted examples of critical information infrastructure are information and communications technology equipment. None the less, Cyber War, ABC media [7] quoted a former CIA & NSA director, General Michael Hayden who held the position that "Infrastructure has always been considered a legitimate target" by terrorists.

4.2 Critical Infrastructures In The Petroleum Sector

Over the past few years, security concerns have been raised about vulnerabilities in key infrastructure. Oil and natural gas utilities are part of the nation's CI. The work of Kevin Hillmer-Pegram, an interdisciplinary PhD candidate at the University of Alaska, Fairbanks itemized five (5) main phases of the activities associated with oil and gas production. They are as follows:

a. Leasing
b. Exploration
c. Development
d. Production and Transportation
e. Decommissioning and abandonment

Each phase involves a complex network of actors from the governmental, private, and civic spheres of the society. Every phase has its associated infrastructure and operations [28]. These critical and strategic facilities often include the:

i. Pipelines
ii. Telecommunications equipment
iii. Reservoirs
iv. Tank farms (mass storage facilities)
v. Power transmission lines
vi. Drill rigs
vii. 3-D seismic survey
viii. Wells
ix. Refineries
x. Offices — corporate, Admin., and control rooms
xi. Industrial control systems, SCADA systems, laptops
xii. Production buildings
xiii. Water-supply systems
xiv. Off-sites utilities and other equipment: surge vessels, boilers, turbines, process heaters, sewer systems.

So, in order to sustain uninterrupted energy production and for quick recovery from major cyber incidents— large oil and gas companies have to bolster their cyber infrastructures to protect their industrial control systems, networks, pipelines, confidential information, exploration and production buildings, telecommunications equipment, tank farms and refineries. This paper agrees with Martin G. J., (2015) who believed that improving the safety of general computing can have an even greater impact on critical information infrastructure safety.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 3, pp: 335-343 www.ijaem.net ISSN: 2395-5252

V. NOTABLE CYBER-ATTACKS INCIDENTS ON PETROLEUM FACILITIES

While physical attacks on pipelines have been more common as we have outlined [17], cyber-attacks on pipeline infrastructures are also becoming more frequent as systems are computerized. The computerization and automation of CIs tend to lead to pervasive cyber interdependencies. The Energy industry faces significant threats, such as hydrocarbon installation terrorism, which can cause plant shutdowns and interruption of utilities. In accordance with the popular maxim by Edmund Burke: 'those who don't know history are destined to repeat history' [9].

5.1. Historic Cyber-attacks On Petroleum Equipment

Incidences abound of cybersecurity threats and attacks, particularly in the oil and gas facilities. Research indicates that companies involved in offshore installations keep a record of past incidents and their impacts in order to avoid reoccurrence and hence, create a better model for properly identifying threats which can occur in the future. The devastating cyber attacks on oil and gas companies in the Middle East in 2012 and again in 2016/2017; the attacks on the Ukrainian power grids in 2015 and 2017 have underscored this increasing risk. Way back in June 1982 even before the internet became ubiquitous, one of the more prominent examples of cyberwarfare—comes from the cold war. A major explosion occurred on the Trans-Siberian gas pipeline. The pipeline's control software unknowingly contained malicious code that massively increased the pipeline pressure that eventually led to the explosion. It created at the time one of the largest non-nuclear explosions in history, so large it was visible from space. The malware was later revealed to be a Trojan horse implanted by the United States in pipeline equipment sold from a Canadian company on to Russia. The end result was an economic sabotage facilitated by computer software [7]

The postgraduate thesis' presentation on Cyber security for critical infrastructures by Ronald. L. Lendvay and Kathleen Kiernan at the Naval Postgraduate School Monterey, California, USA summarized a historic cyber incident. The researchers labeled the June 2012's Stuxnet attack on Iran's Natanz Uranium enrichment facility as the first publicly known use of a cyber-weapon to destroy the critical infrastructure of another country, accomplishing with computer programming, what only used to be possible through bombing or traditional sabotage [37]. Their work further narrated how the worldwide cyber security landscape changed when the presence of that new and sophisticated malware, dubbed "Stuxnet," was discovered in the computers of an Iranian nuclear facility. No doubt, the malware was a cyber weapon, intended to destroy the industrial machinery utilized for uranium enrichment. Another report recorded that Stuxnet computer virus with its highly specialized malicious payload targeted, monitored, hijacked industrial control systems of oil companies in the Middle East (Saudi Aramco in Saudi-Arabia and RasGas in Qatar), including computers used to manage oil refineries and gas pipelines [19].

Night Dragon was another episode launched by attackers with the intent to steal sensitive information such as operational details, exploration research, and financial data from global oil, energy, and petrochemical companies. Whereas the August 15, 2012 cyber-attack [36] was aimed at stopping gas and oil production in the world's largest oil-producing company, Saudi Aramco, Saudi Arabia. Resources flowing to the international markets were impeded—30,000 computers damaged due to virus infection.

Conversely, the cyber incident in Turkey caused an explosion that resulted in the spilling of more than thirty thousand barrels of oil. The potential consequences of a similar attack on the nation's vulnerable critical infrastructures, 2012 Global Risks report says could be devastating. IBM X-Force' 2018 Threat Intelligence Index noted that cyber security does not start and end with technology, with Craig Rogers, et al., 2018 adding that effective identity and access management require 70% people, process and politics and only 30% technology.

The research [39], "the future of cybercrime and security: threats analysis, impacts assessment and mitigation strategies 2019 - 2024 " postulated that the cost per breach will steadily rise in the future. Cybercrime is increasingly sophisticated; the report anticipates that cybercriminals will use artificial intelligence, AI which will learn the behaviour of security systems in a similar way to how cybersecurity firms currently employ the technology to detect abnormal behaviour. Research author Susan Morrow remarked that "All businesses need to be aware of the holistic nature of cybercrime and, in turn, act holistically in their mitigation attempts".

VI. OPERATIONAL AND INFORMATION TECHNOLOGIES ROLES

With CIs becoming progressively cyber-attacks targets, there is great concern to protect these infrastructures owing to the huge losses and impacts of these threats. eSentire, a well-known managed detection and response service provider referenced the Crowd Research Partners' 2018 Cloud Security Report that 43% of organization studied by the firm,

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 3, pp: 335-343 www.ijaem.net ISSN: 2395-5252

acknowledged infrastructure security as their top challenge [20].

6.1 Operational Technology Systems And Workings

Operational technology, OT refers to the hardware and software used to control industrial processes. The traditional OT assets comprise of— Industrial control systems, ICS, process control systems, SCADA systems, and others. Control systems are typically considered operational technology. The ICS monitor, automate, and control critical physical processes, such as physical access control. These control systems typically collect information about facility operations and specific component status (e.g., gate position, reservoir level, hydroelectric generator output, water flow-rate) to checkmate, manage, command, direct, or regulate the behavior of devices or components. Data on component status are sent as electrical signals over digital networks (the Internet and wired/wireless networks inclusive) to control systems and operators. Automated or operator commands may be sent back through the same network to manage operations. However, many of the ICS used today were designed for operability and reliability during an era when there were fewer security concerns than there are today [40].

Attacks on OT could disrupt supply, and trigger a physical event. In August 2017, for instance, a petrochemical company with a plant in Saudi Arabia was hit by a new kind of cyber-assault to sabotage the firm's operations and trigger an explosion. Many operators in energy sector lay emphasis on increase expenditure on the security of their corporate IT systems; this has not been matched for OT systems, thereby leading to their increased attractiveness to cyber assailants [35]. Known cybersecurity risks affecting ICS consist of increased use of digital controls, removable data storage devices, system updates and patches, and insider threats.

6.2 Integrating Info-Tech and Operational Technology For Infrastructural Security

Enterprise information technology (IT or Info-Tech) services consisting of— email, Internet connectivity, Voice over Internet Protocol (VoIP) and telecommunication constitute the emerging enterprise Info-Tech assets. Altogether, computer systems; control systems (e.g., supervisory control and data acquisition, SCADA); networks such as the Internet; and cyber services (e.g., managed security services) are part of cyber infrastructure. Historically, the OT systems were physically isolated from the corporate IT network. In their work for the European Parliament with the theme: "Cyber Security Strategy For The Energy Sector" D. Healey, et al (2016) highlighted the need for integrating the traditional power-related 'hard' assets known as the operational technology (OT) with information technology (IT) – the more business and function-related enterprise assets in the 21st century[15].

At the moment, OT systems are increasingly being connected to corporate networks via the internet, cellular networks or Wireless Fidelity, WiFi and should to be looked at as part of a holistic security framework. Jason Holcomb, (2016) concurred that integrated IT and OT security has become a new trend in this industry. The writer is of the belief that protection against cyber threats requires that the oil and gas industry manages risks (risk management) and adapts to changing technology. Craig Rogers, et al., (2018) likewise advocates for a proactive, holistic, risk-based and well-practiced approach that systematically and rigorously assesses the risks and mitigates them across the enterprises, IT and OT, people and processes[26][11].

VII. IMPACTS OF CYBER-ATTACKS

7.1 The Industry's Most Affected Segments

Repeated cyber intrusions into organizations of all types demonstrate the essence for improved cybersecurity architectures. The risks from cyber-terrorism to the energy supply vary by segments of the industry, which is broadly defined as:

- Exploration and production
- Refining
- Pipeline transportation (liquids)
- Marine transportation
- Products distribution and marketing.

Cybersecurity vulnerability is a weakness or flaw in IT, OT, communications systems or devices, procedures, or internal controls that could be exploited by a threat. According to IDC Energy Insights' security survey, only 50% of oil and gas organizations have a documented and approved information security strategy in place and the same study acknowledges that 40% of oil and gas industry respondents do not know how many security events occurred through applications, devices like removable storage or smart phones, etc. The survey concluded that factors such as enterprise-wide management of information and intelligent, consistent, and integrated information, compliance, information-sharing and use of collaboration tools and technologies are critical capabilities for mitigating risks in TNOCs operations [36]. The online attacks impacts could be of the following groupings or effects:

• Economic impact of destruction or disruption
• Business impact
• Loss of energy supply
• Environment impacts
• Extended repair and recovery time
• Political consequences on public confidence
• Loss of human life (killed or injured)

Cybersecurity attacks disrupt computer systems and networks operations. Data theft, network damage, infiltration and destruction of E-governance, E-sources and E-resources may not be possibly excluded [31]. Managing information infrastructure in a global environment is becoming increasingly complex and the attendant economic impact of cybercrime is huge.

7.2 Financial And Budgetary Implications

The current state of cybersecurity according to Global Oil and Gas Infrastructure Security Market Assessment, a study by Frost and Sullivan predicted that the total oil and gas infrastructure security market is to increase from $18 billion dollars to $31 billion dollars by the year 2021. Despite this spending, the ABI Research study [26] acknowledged that the process control networks in many petroleum companies are "poorly protected against cyber threats and at best, they are secured with IT solutions." It is a statement of fact that offshore oil and gas sector generates around £20 billion of revenue per annum and £12.8 billion of Gross Value Added (GVA) whilst supporting induced, indirect and direct employment of more than 190,000 people; thus, making it one of the key sectors of the UK economy [38]. Over 24 countries [8] sustained an approximate financial loss of $388billion USD to cybercrime in over a period of six years.

Going by 2015 Threat Report of the Australian Cyber Security Centre, covering 2014 and 2015, the Australian CERT (Computer Emergency Response Team) responded to 11,733 incidents, 218 of which involved systems of national interest or critical infrastructure. The government's department of communications confirmed that the average cost of a cybercrime attack to a business is around $276,000 dollars. At the same time, the World Economic Forum's global risks report affirmed that in the United States alone, cyber crime already costs approximately $US100 billion a year. It further emphasized cyber-attacks and threats as one of the most likely high-impact risks [7].

As commerce becomes more reliant on the digital realm, a new report from Juniper Research found that the cost of data breaches will soar from $3 trillion each year to more than $5 trillion in 2024— denoting an average annual growth of 11% [12]. The Cybersecurity Ventures [13] presented the enormous cost that these attacks are having on businesses globally, to the tune of $500 billion per year. It went on to name the banking and financial sectors as top targets in the last five years, with IT and telecom, defence, and the oil and gas sectors trailing closely.

7.3 Governments Efforts And Global Interventions

A pertinent question would be: what are governments doing to support greater security? Since the adoption of the first United Nations resolution addressing cybersecurity in 1999 [34], there have been several multilateral, intergovernmental efforts to deal with cyber insecurity. The European Network Operator organization, ETNO is in agreement that protection of critical infrastructure should be a national responsibility [27]. Even L. Subrananian., et al., (2016), criminology experts and authors of the work "Cyber-Terrorism and Cyber Security: A Global Perspective" also believed that for any type of cybercrime, prevention is considered the best means of response [31].

When it comes to fending off cyber attacks, telecoms operators and Internet service providers, ISPs – being the data carriers, are refutably on the frontline. Johannes Ulrich, chief researcher at a US-based security training and research organization, SANs Institute suggested that attacks would always have to be fought on an ISP level because an end-user or government has little chance of doing so. Likewise, Alan Paller, director of research at same institute agreed that ISPs can enable both the early warning system and the rapid response to certain digital aggressions [27]. This invariably necessitates partnership with ISPs, and telecoms to adequately wrestle online aggressions.

For a developing country like Nigeria, the TNOC companies should see sufficient reasons to sink funds and resources into combating internet-based assaults and demand a minimum level of security and response-time to attacks from ISPs. They must also build reliable cost-effective data protection architecture to improve disaster recovery readiness and simplify management. This can be achieved by requiring each firm to increase their preparedness and improve their cooperation with each other, and by requiring operators of CI and public administrations to adopt appropriate steps to manage security risks and analyze serious incidents [36].

VIII. CONCLUSION AND RECOMMENDATION

These documented attacks demonstrate the importance of robust cyber-security risk assessment plans and schemes that are adequate to counteract actions and intrusions of any kind being perpetrated

by either experienced professionals or amateur hackers.

The works of research author S. Morrow (2019) and security specialist D. Arikpo (2019) summarized our expected security practices as follows:

- Security awareness training of staffs and proper education of the Nigerian populace.
- Frequent systems audits and updates amidst constantly evolving threats.
- Risk assessments plan and vulnerability testing using relevant tools
- Strengthening intelligence gathering by security outfits and
- Establishment of online security unit or a group of skilled personnel in different enterprises.

As security agencies like the 'economic and financial crimes commission' EFCC and the 'independent and corrupt practices and other offences commission' ICPC are working on updating their systems, he stressed that certain legislative measures should likewise be in place for both private and public utility firms that operate in the cyber-ecosystem.

In addition, we should start a cybersecurity program, which may be implemented at either the organization or the function level by integrating activities and leveraging resource investments across the entire enterprise or unit. At the beginning, a security doctrine or an operational concept is defined; threat assessed, and based on the decisions of the Security Committee— a strategy is decided and formalized in a security master plan. Then, planned implementation of the security solutions is done, taking into account the return on cyber security investment.

Moreover, for safety preparedness and quick recovery plans, some experts advocate for proper funding in view of the current cybersecurity arrangement in the industry [5]. An avenue and political neutral environment should be constituted within which governments, oil and gas firms, telecom operators and other stakeholders can consent on the constituents of cyber-attack and agree to undertake greater action towards adoption of state-of-the-art information system for the safeguard of oil facilities. In simple terms, for viable economic growth and social development, establishments should also:

- Organize a cybersecurity program
- Comprehensive legislation and adequate funding
- Adopt state-of-the-art Tech systems.

Consequently, with these incidents consideration of potential cybersecurity risks involved in the energy sector, sufficient defence strategies against online attacks is compulsory for most large national and multinational onshore and offshore oil companies. It is factual that access to cyberspace is essential to social, economic, and political stability [34]; and with the oil and gas sector fueling several aspects of our daily life, the protection of its critical infrastructures is crucial as key driver in nation building.

REFERENCES

[1]. A. Adebola, "Crude Oil Price, Exchange Rate And Macro Economic Performance In Nigeria (1980-2016) Dept. Of Economics, Lagos State University, Lagos, 2017

[2]. A. Caprile, "The effects of oil companies' activities on the environment, health and development in Sub-Saharan Africa" Policy Department Directorate-General For External Policies, EU Parliament, Brussels, 08 Aug., 2011

[3]. Africa Oil And Gas Report "Is Somali piracy on the rebound?" Vol. 18, No 4, June 2017, p13

[4]. A. Madueke, "The future of Nigeria's petroleum industry"Summit 2013, Lagos, 2013, pp. 1-10.

[5]. A. Okafor and A. Olaniyan "Legal and institutional framework for promoting oil pipeline security in Nigeria."Journal Of Sustainable Development, Law and Policy, Vol.8:2, 2017.

[6]. Australian Cyber Security Centre, 2015 Threat Report,2015.Availableatwww.acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf

[7]. A. Wong, "Cybersecurity: Threats, challenges, andopportunities" Australian Computer Society, ACS, Sydney, November 2016.

[8]. B. Hayatudeen, National Cybersecurity Strategy Policy. Abuja, 2015

[9]. Brainy Quotes, Engineering sayings and scenarios.2014Availableat:www.brainyquote.com/quotes/quotes/e/ edmundburk382368.html (accessed March 3rd, 2014).

[10]. CNBC 2015 report "Biggest cybersecurity threatsin2016"www.cnbc.com/2015/12/28/biggest-cybersecurity-threats-in-2016.html

[11]. C. Rogers, M. Bahar, et al. "Responding to the evolving cyber threat landscape in the oil and gas sector" Eversheds Sutherland, Partner, London, October 2018.

[12]. C. Ward, "Businesses losses to cybercrime data breaches to exceed $5 Trillion by 2024" BNP Media, Troy, MI, 28th August 2019. www.securitymaazine.com, accessed 24th September 2019

[13]. Cybersecurity Market Report, Cybersecurity Ventures,2016.www.cybersecurityventures.com/cybersecurity-market-report
[14]. D. Arikpo, "Building capacity against cyber-attacks" and Cybersecurity and cybercrime: As it affects personal and national security" Nigerian Television Authority Intl, NTAi's INSIGHT programmes, 14th & 20th Sept., 2019
[15]. D. Healey, S. Meckler, U. Antia, and E. Cottle Cyber Security Strategy For The Energy Sector" Directorate General For Internal Policies, European Parliament,Brussels, European Union, 2016
[16]. E. Ejoh and P. Okafor "Nigeria loses $100b revenue to pipelines sabotage - Kachikwu" Vanguard Newspapers, February 2017.
[17]. E. J. Byres, "Cyber security and the pipeline control system" Pipeline And Gas Journal, 2009.
[18]. E. O. Yeboah-Boateng, "Cyber-security challenges with SMEs in developing economies: Issues of confidentiality, integrity and availability, CIA." 1st ed., Institut forElektroniske Systemer, Aalborg Universite, 2013.
[19]. Ernst and Young, "Turn risks and opportunities into results. Oil and gas – top 10risks"2013.http://www.ey.com/GL/en/Industries/Oil---Gas/ Turn-risk-and-opportunities-into-results--oil-and-gas--The-top-10-risks. Accessed March 14th, 2014
[20]. eSentire, "Stop the clock: reduce time cyber attackers can target your business" Infograpic, 2019.
[21]. F. Dayo "Diesel power generation: inventories and black carbon emissions in Nigeria" International Bank for Reconstruction and Development, World Bank Group, Washington DC, USA, 2014.
[22]. General Electric, "Cyber Security For Oil And Gas: Helping Mitigate" Risk And Partnering ForASecureFoundation.fromwww.ge.com/digital/products/cyber-security-oil- gas. Accessed on 16th Feb., 2018
[23]. G. K. Saini, M. Halgamuge, P. Sharma and J. S. Purkis "A Review on Cyberattacks: Security Threats and Solution Techniques for Different Applications. Charles Sturt University, Australia, IGI Global., 2019.
[24]. Global Risks Report "From The Dark Side of Connectivity" 2012
[25]. International Monetary Fund, 2011 article IV consultation report on Nigeria. IMF country report No: 12/194, 2012
[26]. J. Holcomb, "Definitive Guide to Cybersecurity for the Oil And Gas Industry" Leidos Commercial Cyber Solutions Group, 2016.
[27]. J. Taaffe "Cyber warfare" Total Telecom, Terrapinn, Holdings ltd, 43 Hatton Garden, London, 2007, pp 15,16
[28]. K. Hillmer-Pegram "A synthesis of existing, planned, and proposed infrastructure and operations supporting oil and gas activities and commercial transportation inArctic Alaska" University of Alaska Fairbanks, 2014. p13
[29]. K. Omeje "Petrobusiness and security threats in the Niger Delta, Nigeria" Africa Centre For Peace And Conflict Studies, The Department Of Peace Studies, University Of Bradford. Current Sociology, Vol 54(3): pp 477 – 499, 2006. Retrieved from csi.sagepub.com at Pennsylvania State University on 19Th Sept., 2016.
[30]. L. LaFronz "Understanding and managing markets in an era of increasing uncertainty" International Oil And Gas Engineer Magazine, Setform Limited, UK, 2013.
[31]. L. Subrananian, J. Liu, and J. Winterdyki Cyber- Terrorism and cyber security:A global perspective" Dept.of Criminology, University of Madras, India.Oct., 2016.
[32]. Merriam-Webster Dictionary, 2019, Incorporated.
[33]. National Cybersecurity Strategy 2019, Dept. of National Security, Prime Minister's office, Spain, Jun. 2019, p18,23
[34]. N. N. Schia, "The cyber frontier: Digitalization of the Global South", European Cybersecurity Journal (2) 2016, pp 82 - 94
[35]. P. Ciepiela "Digitization and cyber disruption in oil and gas" OT/IoT Security And Critical Infrastructure Leader, EYGM Limited, BMC Agency, GA., 2017.
[36]. R. Bigliani, "Reducing risk in oil and gas operations" IDCEnergy Insights, Framingham, MA.,USA, 2013, pp 5,11,12.
[37]. R. L. Lendvay and K. Kiernan "Shadows of Stuxnet: recommendations for U.S. policy on critical infrastructure cyber defense derived from the Stuxnet attack" PG Thesis, Naval Postgraduate School Monterey, California, March, 2016.
[38]. Scottish Enterprise, "A guide to offshore wind and oil and gas capability – a cursory look at industry trends and growth areas" Scottish development international. www.scottish-enterprise.com/~/media/SE/Resources/DocumentsGHI/Guideoffshorewindoilgas.ashx.Accessed on Feb. 25, 2014

[39]. S. Morrow, "The future of cybercrime and security: threats analysis, impacts assessment and mitigation strategies 2019 - 2024" Juniper Research limited, Hampshire, Uk, August 27, 2019
[40]. United States Department of Homeland Security, What Is Critical Infrastructure? Washington, DC: U.S. Dept. of Homeland Security. July 20, 2016.

International Journal of Advances in Engineering and Management
ISSN: 2395-5252

IJAEM

Volume: 02 Issue: 01 DOI: 10.35629/5252

www.ijaem.net
Email id: ijaem.paper@gmail.com