Global Scientific JOURNALS

GSJ: Volume 8, Issue 6, June 2020, Online: ISSN 2320-9186
www.globalscientificjournal.com

EFFECTS OF CYBERCRIME ON OIL AND GAS INDUSTRY

Dorothy Bundi, Mayieka Jared Maranga

Department of Computer Science Meru University of Science and Technology – Kenya
Email: dorriegat@gmail.com

Department of Computer Science and IT, Africa International University – Kenya
Email: marangajared@gmail.com

KeyWords
Cyber-attack, Cybercrime, Cyber espionage, Cyber Security, Cyber threat, Denial of Service (DDoS), Vulnerabilities

ABSTRACT

Cybercrime is among leading causes of loss to numerous offshore oil and gas companies globally. With a yearly loss of millions of monies due to damaged equipment and loss of business, experts claim that cyber-attacks on perilous infrastructure, losses on revenue, environment catastrophic degradation etc. This paper applied exploratory research methodology in reviewing existing literature within this sector with an objective of studying types and forms of cyber-attacks that this industry suffer, the reasons why these attacks are targeted at them and try to suggest ways through which these attacks can be mitigated and/or eliminated. The results of this study show that some of the most common cyber-attacks targeting this sector include Cyber espionage, social engineering, network attacks, phishing, and Brute force attacks. The results can inform cybersecurity specialists and governments in enacting cybercrime frameworks to protect this sector.

1. Introduction

1.1. Background of the study

Cybersecurity is the process by which organizations' information systems are being protected against criminal or unauthorized use of electronic data, or the measures taken to achieve this security state [1]. Cyber security is a subdivision of information security which focuses on defending organizations' computer systems and their associated components such as hardware, software, data, people and networks the underlying digital infrastructure from cyber-attacks, unauthorised access or being damaged or made unavailable. Different data warehouses, websites, software, organizational servers, and accounts can all be exploited through cyber-attacks. The aim of cybersecurity is to protect the companies from unauthorized access or attacks to their data or information that exists in digital or electronic form [2].

In the olden days, Operational Technology (i.e. the hardware and software used to control industrial processes) networks within the oil and gas industry were confined off the internet as opposed to today's desire for efficiency and real-time decision-making which removes that freedom. A cyber-attack on an Operational Technology environment can have grave results including prolonged outages of services via denial of service attacks, damage to the environment and even loss of life [3].

Cyber-attacks can either be active attacks or passive attacks based on the intensions and motive of the attacker. Cyber threats aim at compromising the cybersecurity that the company has put in place with an aim to launch a cyber-attack [4]. There exist several highly skilled and motivated enemies that are actively looking for an opportunity to exploit any small security vulnerability in the operational technology networks, the process control systems and critical setup of oil and gas industry firms. They are usually motivated by the economic benefits as well as espionage, malicious disruption of processes and destruction among other motivations

[5]. While numerous operators in the oil and gas and related businesses have recognized the need to upsurge emphasis and expenditure on the security of their corporate information technology systems, they have not matched these efforts to the efforts directed to the security of the operational technology systems [6]. This has led to their amplified appeal to cyber-attacks.

Recently, cyber threats and cyber-attacks directed towards oil and gas industry pose a progressively puzzling problem for economic competitiveness of any nation and the globe in general [7]. The oil and gas industry are a mainly attractive target for cybercrime and their associated havoc. As pointed out earlier above, this is mainly because there are several weak points of entry for attackers, there are more adversaries wanting to cause turmoil, and most importantly, there is more potential for utter disaster. For instance, if a retailer suffers a cyber-attack, largely, customers' personal data may be compromised, but if the attackers can gain access to the systems of an oil and gas installation, the repercussion is likely to be much more severe [8].

Cyber-attacks usually take different forms, ranging from cyber espionage by foreign intelligence services to attempts to interrupt a company's operations. These threats have grown more sophisticated over time, making them more difficult to detect and defend against. The attackers have also evolved from solitary hackers with few & uncomplicated resources to state-sponsored squads of programming whizzes. Numerous major oil and gas producers of the world including officially the Saudi Arabian Oil Company, Qatar's RasGas, etc. have fallen victim to cyber-attacks. Other companies such as Chevron among others in Middle East and United States have also had their networks affected and infected in one way or another. Significant damage has been done in several of these corporations, but the cost of future attacks might be much higher [9].

These attacks are largely targeted on corporate assets, public oil infrastructure, or the larger economy through energy prices. Successful cyber-attacks portend danger to the competitiveness of the oil and gas industry. This is one of the industries that are most technically advanced and economically important sectors of any nation especially the oil manufacturing nations. While most intrusions on oil and gas industry have been previously concentrated on theft of intellectual property and business trade secrets, the malware attacks on oil companies are reflecting a worrying change towards attacks intended at cause physical disruptions and financial loss to the organizations operating in this industry [10].

1.2. Problem Statement

The oil and gas (O&G) industry has changed substantially over the last decade. The greater connectivity of the digital age and the Internet of Things (IoT) has resulted in increased efficiency through big data, analytics, sensors, and the ability to automate highly sensitive tasks. However, it has also opened the doors to cyber-attacks. The O&G sector is no longer protected by isolated control systems and detached core operations meaning that cyber security will be a major area of investment for O&G organisations [5].

According to [10] the rise in the cybercrime cases targeting the oil and gas companies are also attributed to the high dependency on information systems that are hosted in the cloud. These companies typically run sprawling operations with sites in hard-to-reach locations. Remote monitoring for performance, quality control and safety is therefore essential, but with bandwidth limitations and the focus on availability, communications are often left unencrypted.

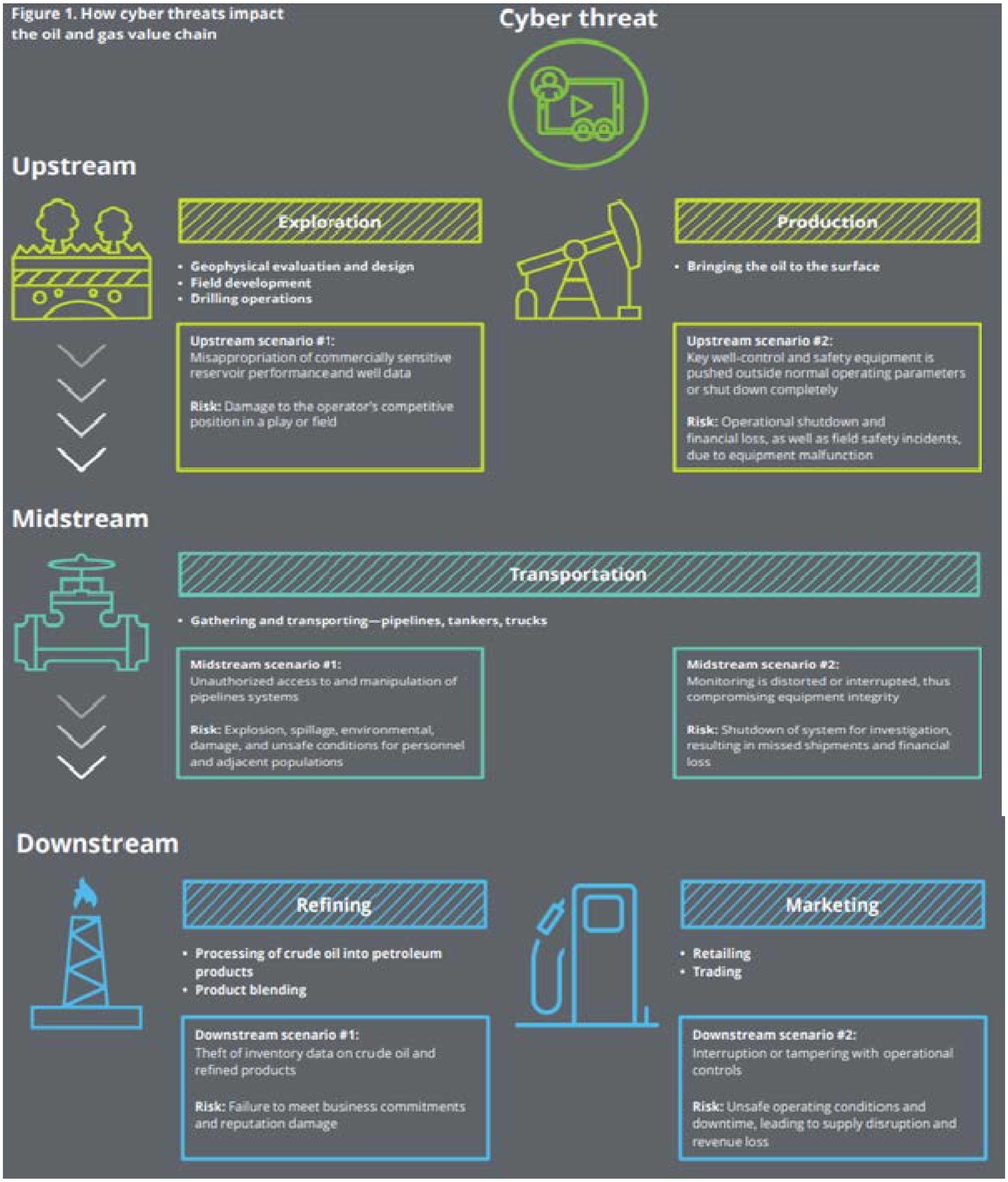
This paper intends to study the types and forms of cyber-attacks that oil and gas industry face, why these attacks are targeted the companies operating in the O&G industry and the results of the study are used to suggest ways through which these attacks can be mitigated or eliminated.

2. Related Literature

2.1. The Nature of Oil and Gas Cyber Threats

The attackers behind cyber-attacks on the oil and gas industry and related firms differ just like their objectives and methods. International intelligence and defence organizations, organized offenders and other non-state individuals and ad hoc hackers have all been connected to penetrations against private-sector subjects containing energy corporations [7]. Similarly, the insiders - those with confidential access to the corporation's computer network - such as past employees or current employees or authorized contractors. The methods that invaders use against oil and gas organizations are developing, as are the defence methods used by these organizations [11].

Several Progressive & insistent threats are other problem for the O&G industry in which groups attempt to steal data and information that can contribute to the sponsoring administration in ensuring national and economic security. Theft of data and information will most likely focus on information related to natural resources exploration and energy deals. Progressive & insistent threat groups are also engaging in destructive and disruptive actions against the energy industry especially in areas experiencing conflict such as Middle East and northern Africa. In these areas, hackers opportunistically target oil and gas companies in response to supposed disagreements. Usually, these attackers conduct a wide distributed denial of service (DDoS) attacks on the systems of these industries, they deface these companies' websites, or steal and expose secluded and confidential information of these companies in an attempt to humiliate the companies and gain attention for their intended cause [12]. The cyber threats categories are divided into upstream, midstream and downstream threats as shown in the figure 1 below:



- Geophysical evaluation and design
- Field development
- Drilling operations

- Bringing the oil to the surface

Upstream scenario #1: Misappropriation of commercially sensitive reservoir performanceand well data

Risk: Damage to the operator's competitive position in a play or field

Upstream scenario #2: Key well-control and safety equipment is pushed outside normal operating parameters or shut down completely

Risk: Operational shutdown and financial loss, as well as field safety incidents, due to equipment malfunction

- Gathering and transporting—pipelines, tankers, trucks

Midstream scenario #1: Unauthorized access to and manipulation of pipelines systems

Risk: Explosion, spillage, environmental, damage, and unsafe conditions for personnel and adjacent populations

Midstream scenario #2: Monitoring is distorted or interrupted, thus compromising equipment integrity

Risk: Shutdown of system for investigation, resulting in missed shipments and financial loss

- Processing of crude oil into petroleum products
- Product blending

- Retailing
- Trading

Downstream scenario #1: Theft of inventory data on crude oil and refined products

Risk: Failure to meet business commitments and reputation damage

Downstream scenario #2: Interruption or tampering with operational controls

Risk: Unsafe operating conditions and downtime, leading to supply disruption and revenue loss

Figure 1: The Cyber Threat Upstream, Midstream & Downstream (Adapted from Deloitte report: An integrated approach to combat cyber risk) [7]

2.2. Cyber Threats to Oil and Gas Industry

Cyber threats to oil and gas industry can be in various categories, including:

2.1.1. Cyber espionage

Cyber espionage is a form of cyber-attack which involves stealing of classified and sensitive data/information or intellectual property such as trade secrets, national secrets, etc. to gain an advantage over a competitor organization or government or target company. Cyber espionage therefore comprises of third parties who attempt to secretly seize an organization's sensitive internal communiqué or data/information with the intention of collecting commercial intelligence. For years now, oil and gas corporations have been vulnerable to this kind of exploitation mainly because their operations have been increasingly becoming dependent on information that is largely digitally transmitted. The revelation of copyrighted data/information can weaken a company compared to its peer companies and even endanger its existence over time [13].

The spies in this case are militias of despicable hackers from all over the world who practice cyber warfare for partisan, economic, **or** military gain [14]. These comprise of intentionally conscripted and greatly valued cybercriminals who possess technical skills to shut down systems and networks ranging from government infrastructure to oil and gas systems, to financial software or any other utility resources. Through these kinds of espionage, the attackers have previously influenced the aftermath of political ballot votes, created disorder at international happenings, and aided businesses to succeed or fail [15]. Many of these cybercriminals implement advanced persistent threats (APTs) as their main mode of operation to sneakily infiltrate targeted networks or systems and stay undetected for a long time that usually can span to years.

Oil and gas firms in the United States of America have been subject to frequent and habitually successful espionage attempts by either insiders, competitors, or foreign agents with the aim of accessing their trade secrets such as long-term strategies, tenders made for new drilling size and private consultations with foreign executives relating to oil and gas. According to industry reports, these cyber espionage criminals have often been successful in accessing the organizations' manuals and geologic data [16]. Numerous other corporations have most likely fallen victim to these attacks without ever realizing it. One of the most successful recognized crusades against the American oil and gas companies is the one nicknamed "Night Dragon" by McAfee. Night Dragon remained a well "coordinated, secret, and directed" campaign by hackers based in China to acquire confidential data/information from five main western energy enterprises. This started at around the year 2008 and extended into early 2011. This attack was able to acquire several gigabytes of highly sensitive content comprising copyrighted data/information relating to oil and gas ground procedures, associated financial transactions, and bidding data [17]. It is however quite challenging to illustrate how the acquired data/ information were used. One oil executive who was later interviewed said that he believed that on some instance a competing oil company seemed to know his company's bidding strategies beforehand towards a lease auction that was scheduled which resulted in his company losing the bid [8]. Security specialists believe that Night Dragon attack is one of the numerous comparable attacks that oil and gas firms aren't unaware about or are afraid to reveal in public for dreading offending financiers [2].

Another example of espionage attack is the new lyceum APT that is targeting oil and gas firms in the Middle East, and across Africa and Asia. The cyber-espionage scene in the Middle East is getting more congested as of the year 2019 especially with the unearthing of hackers that has been targeting oil companies in that region ever since mid-2018. These hacks followed a simple but very effective pattern where initially, Lyceum attackers exploit techniques such as password spraying and brute-force attacks to crack targeted specific email accounts at oil and gas companies [9]. Once successful, the attackers get to the second phase where the Lyceum hackers use those compromised email accounts to spear-phish the intended victim's co-workers. These phishing emails delivered malicious Excel files which try to infect computer/electronic users/devices in the same company with malware.

The main targets of this stage of spear-phishing crusade include the top executives, the Hunan Resources staff, and the Information Technology personnel in the same company [17]. The contaminated excel files usually contain a DanDrop payload, which infect the victim computers with a remote access Trojan called DanBot. The Lyceum attackers then use the remote access Trojan to transmit additional malware on target systems. Cyber security experts argue that they do not have enough evidence to link Lyceum to a specific nation. Equally, the attackers' concentration is anticipated on remaining on the oil and gas industry which is largely financially lucrative to most cyber-espionage hackers that target the Middle East [9].

2.1.2. Disruption of critical business operations by attacks on networks

Another key threat confronting the oil and gas firms is the disruption of precarious physical operations by cybercriminals in the cyberspace. With the advancement of information technology and its application in different phases of oil and gas making i.e. beginning at oil and gas exploration and production to their processing and distribution, the vulnerability of these industry operations also increases especially to the cyber-attacks.

A cybercriminal with advanced tools, access rights, and with the right knowledge may, for instance, ascertain critical supervisory control and data acquisition systems together with the industrial control systems that are used to run critical oil and gas infrastructure which may be connected to the Internet [5].

Once these attackers get into the system, could are theory likely to start the flow of natural gas or oil over a pipeline to stop then possibly activate an explosion at petrochemical facilities (terrorism) or damage offshore drilling rigs which may lead to oil spills which becomes dangerous in case of fire or cause environmental destruction, outages of energy-supply and even the loss of life [8].

2.1.3. Social Engineering

This is the form of threat that aims at compromising the company's cybersecurity using the employees who are the weakest point of any security. The attacker relies on human interaction to trick users into breaking security procedures in order to gain sensitive information that is typically protected [4]. Systems controls and employees need to learn to be suspicious and recognize such attacks as they are happening. Oil and Gas Company's management should ask basic questions to get a sense of the company's vulnerability [13]. Can anyone gain unauthorized physical access to the company's office or to the executives' e-mail or pretend to be sending messages from their e-mail accounts? Retrieve and modify the source code that runs the company's key products? Access the company's data centre? Employee security education is one of the major ways to prevent cyber threats which should be embraced by the oil and gas companies' management [18].

Therefore, social engineering is seen as the cornerstone and initial point for just about every other targeted attack in the oil and gas industry and indeed any other industry that is susceptible to cyber-attacks. Hackers scrutinize social media sites of the associated companies' staff as well as different online forums including company directories and other sources of intelligence obtainable to them as they look for an advantage that will help them get past the initial security such as firewalls, or at least get past the network perimeter [19].

3. Methodology

This paper uses exploratory research design with an objective to review existing literature and secondary data based on the latest publications and technologies available on the effects of cyber-attacks on oil and gas industries. This research design was guided by the following research questions:

i. What are the types and forms of cyber-attacks that oil and gas industry face?

ii. Why these cyber-attacks are targeted to the companies operating in the oil and gas industry?

iii. What ways through which these cyber-attacks can be mitigated or eliminated?

The researcher conducted the advanced search for the relevant publications from the electronic libraries and databases using the query string(s) defined below:

(Cyber-attacks OR "Cyber threat" OR "Cybersecurity") AND (Oil OR Gas OR Oil* OR *Gas*)

Some of the electronic databases and electronic libraries that were searched by the authors include: Google Scholar, IEEE-Xplore, Elsevier Science Direct, Mendeley, Springer link and ACM Digital Library.

4. Results and Discussions

4.1. Top Cyber Security Vulnerabilities for the Oil and Gas Industry and their Mitigation

While organizations continue to prioritize cybersecurity - and are making good progress in identifying and resolving vulnerabilities - they are more worried than ever about the breadth and complexity of the threat landscape.

To a lager extent, especially in large scale oil and gas producers, Industrial computerization including the implementation of control and safety systems is a phenomenon that if witnessed in the oil and gas industry. The firms in this industry are largely digitized and fairly dependent on digital equipment [20]. Previously, these systems were exclusive but now, to a large extent, they are based on commercially available components such as computers with Microsoft Windows operating system. This implies that commonly well-known vulnerabilities of such standard products will also be visible in the industry.

Equally, in the previous days, the interconnection between process apparatus and control systems were isolated and proprietary unlike nowadays where they are based on Internet technology. Industrial computerization and control systems were previously kept physically separate from typical information systems and the associated open networks. The desire to transmit data from production stage to the information systems coupled with the desire for provision of remote maintenance drives organizations away from such separation because it will be practically impossible. Equally, there is a rise in the use of remote control from an onshore location which usually demands the use and application of common computer networks. Ultimately, this implies expo**sure of the production** equipment to network and internet related vulnerabilities.

According to [6] report which is one of the Global Information Security Survey that investigates the most important cybersecurity issues facing organizations today. It captures the responses of nearly 1,200 participants around the globe from over 20 industries. This paper bases the findings and conclusions on those insights and the extensive global experience of working with clients to help them improve their cybersecurity programs in various sectors.

The following findings are from the 40 participants from the oil and gas (O&G) sector as indicated by the Microsoft report [6].

a. Employee awareness remains important

- 78% of the respondents consider a careless member of staff as the most likely source of a cyber- attack.
- 43% of the respondents stated that significant cyber breaches are from a lack of end user awareness, exploited via phishing.

b. Information security needs board-level attention

- 87% have not fully considered the information security implications of their current strategy and plans.
- 46% feel the whole board is knowledgeable about information security.

c. The risk to reputation is rising

- 60% have had a recent significant cybersecurity incident.
- 15% have a robust incident response program and regularly conduct table-top exercises.

d. A skilled cyber workforce is essential to keep pace with evolving threats

- 50% say the lack of skilled resources is challenging information security's contribution and value to the organization.
- 95% say their cybersecurity function does not fully meet their organization's needs.

e. Challenges are on the rise with the Internet of Things (IoT)

- 17% feel it is very likely that they would detect a sophisticated cyber-attack.
- 48% say it will be challenging to ensure that the implemented security controls are meeting the requirements of today.

f. The financial impact of breaches is not fully examined

- 97% of the organizations' information security reports do not evaluate financial impact of every significant breach.

- 63% would not increase their cybersecurity spending after experiencing a breach that did

In summary, the following are some of the vulnerabilities facing the oil and gas industry across the globe according to [6]:

i. Lack of or limited cyber security awareness and training among oil and gas stakeholders. This has mainly been compounded by a long tern thinking that cyber security is a preserve of Information Technology and computer science individuals. Whereas these are the individuals that would protect these spaces, they are not monopolies to the ideas and knowhow related to computer security.

ii. Rampant remote connection and operations and maintenance especially of the oil and gas equipment. As pointed out earlier, this I likely to expose the equipment to the attackers. There is therefore reason to insist on onsite access and maintenance of these systems.

iii. Tendency to use standard Information Technology products. These products and software have already known weaknesses and so makes it possible for attackers to take advantage of the vulnerabilities to gain access to the oil and gas systems. Instead of standard information systems, oil and gas industry should invest in proprietary and customised systems which will have limited exposure to the cyber-attackers mainly because their vulnerabilities are not so common. There is also reason to conduct frequent penetration tests to ascertain the points of weakness in their systems and provide necessary patches frequently to seal the weaknesses.

iv. Staying pretty with inadequate cyber security culture within the whole supply chain of oil and gas industry including producers, vendors, suppliers, and contractors etc. Most of the associated individuals have a culture of trusting and so fail to frequently update themselves against cyber-attacks.

v. Insufficient separation networks. This means, the more organizations want to make their information technology systems interlinked with industrial systems, the more the oil and gas control systems are likely to be exposed to the cybercriminals. There is therefore need to separate industry control and production systems from the usual information systems. Data can be imported from the production systems to the information systems where necessary without interlinking the two.

vi. The increasing use of mobile devices and mobile storage units including PDAs, IPADs, smartphones etc. There is need to restrict the devices used to access industrial systems and networks. The Bring Your Own Device (BYOD) policy by many other organizations is dangerous especially in managing access control.

vii. Data networks between offshore and onshore facilities, unless proper security like offering secure channels, data transmission between no-show and offshore sites will remain dangerous. The need for this data is so crucial that it somehow must be shared between the different sites.

viii. There is also claims of these firms I this industry possessing insufficient physical security of data rooms, cabinets, among others. This makes it a little easy for attackers to physically break into the facilities hosting some critical systems. There is therefore reason to ensure proper and comprehensive physical security in all areas of oil and gas firms.

ix. Overreliance in vulnerable software is also another challenge. Most of these firms do not want to invest in proprietary and domesticated software. The vulnerable software and components being used will keep on exposing the industry to attacks.

x. Consistent use of out-dated and ageing control systems in oil and gas facilities. These systems are regarded as legacy systems. Changing them has been resisted over time. Therefore, attackers keep on learning their points of weakness for a long time which increases their chances of penetration.

4.2. Mitigating Cyber Threats and Cyber attacks

i. Understand the sources of the threats. The beginning of cybercrime saw stand-alone cybercriminals working on their own personal aims. However, gone are those days and different countries have “wised up” to reap the perceived benefits of cyber espionage and oil and gas industry is a big catch. If different corporations understand the sources of their attacks, they are most likely going to understand how to defend themselves.

ii. Discover the attacker’s motive. By understanding the threat sources can provide guidance towards discovering the motive of the espionage hackers. These motives are likely to range from attempt to gaining corporate competitive advantage to system disrupting in an organization or region. The motives of such attacks often indicate the method used to hack. Therefore, when the hacking methods are identified, there is a likely greater understanding of the target system hence leading to an enhanced understanding of the method that will most likely be used to penetrate organizational systems.

iii. Employ thoughts like those of a hacker. To get hold of cybercriminals accidentally happen. Therefore, thinking like a hacker is likely to offer the organization indication of what the hackers' movements are. Thinking like this should be a norm in an endeavour to protect an organization as opposed to doing it as an aftermath of a breach. Should the company's cyber security squad get into the mind-set of the hacker(s), they will be able to actively look for their own vulnerabilities and comprehend necessary tactics to be used to gain entry and what data/information can be accessed using the discovered methods.

iv. Develop a proactive approach. Proactive approach to cyber security is usually an effective way of cyber protection. There is a saying that "best defense is implementing good offense" which really makes a lot of sense now and someone once said, "it is now time to start thinking like a bad guy and fight back."

v. Implement data security frameworks and techniques such as data encryption, intrusion detection and intrusion prevention techniques etc.

4.3. An Integrated Approach to Combat Cyber Risk and Securing Operations in Oil and Gas

The oil and gas industry are advancing towards digitization, robotics, and the Internet of Things (IoT) among other technological evolution. These concepts are speedily being incorporated into the operative atmosphere of oil and gas industry. Equally, the interest of cyber criminals in the industrial operations of oil and gas industry has increased over time subsequently leading to cyber-attacks that have largely compromised both production and safety of this sector. To implement an integrated approach, there is need to:

i. Building a unified program

For a long time now, the primary motivation behind designing and deploying security controls for physical production processes especially in oil and gas industry has been done to ensure safety. With all these efforts, the scenery of potential attacks now is around the cyber space. These therefore require a unified program to address oil and gas cyber security in a systematic manner across all industry operations by ensuring security, resiliency, and vigilant industrial systems

a. Secure Industrial Systems

This is about preventing system penetrations or compromises by implementing effective and automated controls and monitoring. It is however not possible to fully secure an information system. But even then, critical assets and infrastructure, and their associated industrial Control Systems, should be in the top of the list. The whole supply chains and its processes should be secured, and its weaknesses mitigated from end-to-end.

b. Vigilant Industrial Systems

Continuous monitoring of the industrial control systems in the oil and gas industry in addition to security will determine their system's security. Valuable efforts towards vigilance begin with knowing what needs to be defended against. There are numerous evident threat trends in the oil and gas industry, which can provide a decent starting point for understanding the types of attacks targeting industrial control systems. These trends supplemented by a good understanding of the industry's risks will help predict what might occur and so be able to design detection and prevention systems accordingly.

c. Resilient Industrial Systems

A resilient system should identify potential cyber-attacks, neutralize them, and rapidly restore normal organizational processes. This generally involves detection, response, and recovery. At any specific point of the oil and gas value chain, whether upstream operations, midstream processing plants and pipelines, or downstream refining and delivery logistics, continuous monitoring of equipment should allow real-time detection of any anomalies. This comprises of continually understanding the status of oil and gas pumps, compressors, valves, and process units, including rates of flow and fluid and gas patterns. Continuous visibility and resilience will facilitate rapid reaction to any attacks to eradicate environmental hazards.

ii. Implement key controls

To be able to implement controls that are necessary to cyber security, there are several pillars necessary to transform cyber security in an information security systems environment of Oil and Gas Companies. By implementing these controls, the companies will be able to provide basic security that will aid in achieving security, vigilance, and resiliency. These basic controls include:

a. Awareness training: there is need to enforce mechanisms that will ensure cyber security awareness in these companies together with thorough training meant to offer all employees and management the essential skills for interacting with systems in a safe, secure, and responsible manner.

b. Access control: Information security system components which include hardware, software applications, and computer networks, should be physically and logically secured by enforcing access control mechanism that will ensure that access is only granted to an individual after strict authentication and authorization has been established.

c. Network security: Access to cable and wireless computer networks within the information security system environment of Oil and Gas industry should be restricted and secured in accordance with top notch identity and access management tenets which could include dynamic provisioning and authentication of users, all time monitoring, and end point security.

d. Portable media: Use of portable media (the Bring Your Own Device (BYOD)) into the information security systems environment of Oil and Gas industry should restricted and thoroughly scanned for malicious software.

e. Incident response: Incident management policies should be developed by implementing such mechanisms such as intrusion detection and carry out penetration tests periodically. This will help detect points of weakness hence be able to provide holistic defense.

iii. Embrace good governance

The management of the oil and gas companies can consider including cybersecurity in the policies and procedures that govern the day to day operations and business processes of the companies

Conclusion

Sustained low oil prices are driving the adoption of digitization across the oil and gas industry, ramping up the stakes for cybersecurity. Responses to cyber-attacks must be multi-layered, repelling the most common attacks, with a nuanced approach for advanced and emerging threat vectors in the oil and gas sector. To protect critical information, an oil and gas organization must not only address the security of the traditional ICT environments, it must also deal with the added complexities from the innovative digital business process disruptors, such as robotic process automation, IoTs, blockchain and artificial intelligence. Never before, has it been so important to ensure that security efforts are integrated into every facet of an oil and gas organizations operations, which we call “cyber fusion.”

Defending against common attack methods means point solutions remain a key element of cybersecurity resilience, with tools including antivirus software, intruder detection and protection systems (IDS and IPS), consistent patch management and encryption technologies to protect the integrity of data, even if an attacker does gain access to it. Employee awareness is also a crucial frontline defense, building cybersecurity consciousness and password discipline to protect against the relentless malware and phishing campaigns.

Defending against advanced attacks means accepting that attackers will get in and being able to identify intrusions quickly. A Security Operations Center (SOC) that sits at the heart of the organization’s cyber threat detection and response capability is an excellent starting point, providing a centralized, structured, and coordinating hub for all cybersecurity activities. SOCs are increasingly moving beyond passive cybersecurity practices into active defense - a deliberately planned and continuously executed campaign that aims to identify and remove hidden attackers and defeat likely threat scenarios targeting the organization’s most critical assets.

Defending against emerging attacks, such as the rise in cyber-physical threats, means recognizing that some threats will be unknown, especially in the oil and gas sector, where many are still in the early stages of their digital transformation journeys. Organizations need to build agility into their cybersecurity practices and approaches so that they can react quickly when the time comes. Organizations with good governance processes underlying their operational cyber fusion approach can practice security-by-design - building systems and processes able to respond to unexpected risks and emerging dangers.

Acknowledgment

The authors would like to thank our family members, workmates, and everyone who aided in the success of this research.

References

[1] L. Morris and M. Ma, "The Agile Innovation Master Plan," vol. 13, no. 1, p. 356, 2017.

[2] N. Heard, N. Adams, P. Rubin-Delanchy, and M. Turcotte, "Data Science for Cyber-Security by Nick Heard, Niall Adams;Patrick Rubin-Delanchy;Melissa Turcotte | PDF, eBook | Read online," Amazon Books, 2018. [Online]. Available: https://www.perlego.com/book/845262/data-science-for-cybersecurity-pdf. [Accessed: 11-May-2020].

[3] O. Eunice, B. Dorothy, and O. Omosa, "The Impact of Cyber Attacks on E-Businesses," IJCSN-International J. Comput. Sci. Netw., vol. 8, no. 4, pp. 354–357, 2019.

[4] Cisco, "Cisco 2016 Annual Security Report," Cisco Annu. Rep., pp. 1–87, 2016.

[5] E. A. Fischer, "Cybersecurity Issues and Challenges: In Brief," Congr. Res. Serv., pp. 1–12, 2016.

[6] Microsoft, "cyber threat landscape in the Oil and Gas Secor Report," no. October, 2018.

[7] B. K. Rick and K. Iyer, "Countering the Threat of CyberAttacks in Oil and Gas," 2015.

[8] H. Kazan, "Contemporary Issues in Cybersecurity," J. Cybersecurity Res., vol. 1, no. 1, p. 1, 2016.

[9] C. Cimpanu, "A cyber-espionage group has been stealing files from the Venezuelan military | ZDNet," 2019. [Online]. Available: https://www.zdnet.com/article/a-cyber-espionage-group-has-been-stealing-files-from-the-venezuelan-military/. [Accessed: 14-May-2020].

[10] Jason Holcomb, "Definitive Guide to Cybersecurity for the Oil &amp; Gas Industry," 2016.

[11] J. Blice, "Oil and Gas Cyberthreats," 2019. [Online]. Available: https://www.mossadams.com/articles/2019/november/dangerous-oil-and-gas-cyberthreats. [Accessed: 14-May-2020].

[12] V. Patil, C. Patil, and R. N. Awale, "Security challenges in software defined network and their solutions," 8th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2017, 2017.

[13] C. Black, "What is Cyber Espionage? | Cyber Espionage Definition | VMware Carbon Black," 2018. [Online]. Available: https://www.carbonblack.com/resources/definitions/what-is-cyber-espionage/. [Accessed: 14-May-2020].

[14] P. Ciepiela, "Digitization and cyber disruption in oil and gas," pp. 1–16, 2017.

[15] E. Segal, "Secure Coding: How to Prevent Vulnerabilities from Creeping into Your Software | Codementor," 2019. [Online]. Available: https://www.codementor.io/eddiesegal5/secure-coding-how-to-prevent-vulnerabilities-from-creeping-into-your-software-xn487opv8. [Accessed: 05-Dec-2019].

[16] B. Clayton and A. Segal, "Addressing cyber threats to oil and gas suppliers," Une, vol. 201, no. June, p. 3, 2013.

[17] N. Hodge and A. Entous, "Oil Firms Hit by Hackers From China, Report Says - WSJ," 2011. [Online]. Available: https://www.wsj.com/articles/SB10001424052748703716904576134661111518864. [Accessed: 14-May-2020].

[18] J. Kambic, K. Aurthor, M. Horner, T. Jensen, K. Johansen, and B. Lee, "Crude Faus: An Analysis of Cyber Conflict within the Oil & Gas Industries," Cerias Tech Rep. 2013-9, pp. 1–36, 2013.

[19] A. H. Hajirezaie, S. Aydin, L. Sassan, and N. A. Menad, "Applications of Artificial Intelligence Techniques in the Petroleum Industry - Hemmati Sarapardeh, Abdolhossein, Larestani, Aydin, Menad, Nait Amar, Hajirezaie, Sassan - Livres," 2020. [Online]. Available: https://www.amazon.fr/Applications-Artificial-Intelligence-Techniques-Petroleum/dp/0128186801. [Accessed: 14-May-2020].

[20] R. Sloan and R. Warner, "Software Vulnerabilities," Unauthorized Access, pp. 157–180, 2013.