COUNTERING CYBER THREATS IN OFFSHORE OPERATIONS OF SMART FIELDS: A SURVEY

Sonny N. Epelle¹ and Bunakiye R. Japheth²

¹Department of Computer Science, Ignatius Ajuru University of Education, Rivers State, Nigeria
²Department of Computer Science, Niger Delta University, Bayelsa State, Nigeria
Email: ¹epelleson@gmail.com, ²bunakiye.japheth@ndu.edu.ng

Abstract
The significance of offshore petroleum in providing the world’s energy demands cannot be over overstated. The growing global energy resources demand, along with considerable technological developments, has resulted in a dramatic transfer of petroleum operations from onshore to offshore locations. States and oil companies are looking to the sea for offshore petroleum resources more than ever before. The offshore industry accounts for roughly 30% of overall petroleum output. This figure is likely to rise dramatically due to declining onshore fields and rapidly rising offshore petroleum exploration and development. The digitization of operational procedures in the oil and gas industry has created new potential to increase productivity and reduce costs. This, however, has also exposed the organization to a wide range of new cyber threats. For many years, the upstream sector, particularly offshore oil installations, has been an attractive target for terrorists. Attacks on crude oil and natural gas (O&G) firms have increased in frequency, sophistication, and impact as the industry adopts more linked technologies. As hackers’ motivations evolve - from cyberterrorism to industrial espionage to interrupting operations to stealing field data - and firms increasingly relying daily operations on linked technology, dangers and stakes are rising rapidly. As a result, the sector must be protected from ongoing threats. This study therefore aims at looking at ways to Countering Cyber Threats in Offshore Operations of Digital Oil Fields. Organisations can fight sophisticated hackers by anticipating assaults, reacting in real time, and securing assets depending on their worth. They must use the “active defence” approach by taking all steps geared at predicting, detecting, redirecting, and isolating cyberattacks, if they must keep their organization secured.

Keywords: Energy Resources Demand, Appealing Targets for Terrorism, Digital Oil Fields, Digitization, Cyber Threats, Mitigation

Sonny N. Epelle and Bunakiye R. Japheth(2022), Countering cyber threats in offshore operations of smart fields: A survey
© Afr. J. Comp. & ICT, September 2021; P-ISSN 2006-1781
1. Introduction

The oil and gas system has an impact on every part of the country, and its operation is dependent on a sophisticated network of instrumentation, control, communications, and human and commercial activities. Increased control capabilities have resulted in increased system efficiency. However, as we become more reliant on technology and web-based communication, serious cyber security threats have emerged. With the oil and gas sector fueling practically every part of our daily lives, it's never been more important to protect this vital infrastructure. We can't afford to overlook the impact of cyber-attacks on the operations and systems that support our way of life. As a result, this study will take a closer look at the attraction of these vital infrastructures to cyber-attacks and their vulnerabilities, as well as provide solutions for countering cyber threats, particularly in the context of Digital Oil Fields' offshore operations. The aim of this study therefore, is to examine ways of countering cyber threats in offshore operations of Smart fields. Offshore petroleum plays a critical role in meeting the world's energy needs. The increasing global demand for energy resources, coupled with increased technological innovations, has resulted in a significant shift of petroleum operations from onshore to offshore locations[1]. More than ever before, states and oil companies are looking to the sea for offshore petroleum resources [2]. About 30% of total petroleum output comes from the offshore sector [3]. Due to declining onshore resources and rapidly developing offshore petroleum exploration and development, this number is likely to climb significantly[1, 4].

In the oil and gas industry, digitization of operational procedures has opened up new possibilities for increasing efficiency and lowering costs. In contrast, the company has been exposed to a new set of cyber threats as a result of the convergence of operational and business systems [5]. Digital Oil Field (DOF), is all about how oil fields are run. By connecting remote sites in real-time to enable collaborative working, better decisions can be made, health risks can be reduced, Health Safety and Environment (HSE) can be improved, operating costs can be reduced, and output can be increased. DOF would not have been possible without smart field devices, the integration of industry automation systems, the integration of the Industrial Control System (ICS) with corporations networks/systems, and the capture of real-time data [6]. DOF automation systems are similar in nature to IT systems used in enterprise networks, and they have become vulnerable to similar cyber attacks targeted at enterprise systems. Cyber security threats of today has transformed beyond the basic spread of viruses, computer data loss, and data theft, to the nature and ability to alter process plant operations such as increasing pressure in a pipeline, changing field device parameter settings, closing/opening a motorised valve, and causing a Denial of Service (DoS) attack within ICS, increasing/decreasing motor speed, showing a fictional process diagram, and flashing alerts on operators' Human Machine Interfaces (HMI) [6]. Modern automation systems, according to AL-Issa [6], are based on industry standards like Windows or TCP/IP. As a result, they were vulnerable to cyber threats comparable to those that impact corporate business networks' systems. The consequences of cyber-attacks on industrial vital infrastructures, on the other hand, are dangerous, hence cyber security defenses and considerations must be built into critical infrastructure cyber security plans. Note that cyber security risks to vital infrastructure and/or the environment may result in loss of life, view, control, operation, production or damage to critical infrastructure and/or environment. The automation technologies and the digital oilfield have made drilling rigs and all onboard equipments considerably more networked than before. The old isolation concept for drilling rigs is no longer sufficient to protect them from cyber-attacks. Remote access to a variety of shore-based facilities is common on rigs, whether for real-time operations support or equipment troubleshooting[7]. Furthermore, there is a growing trend to locate control centers onshore, with one control center serving many fields, which may introduce vulnerability. Wireless technology is increasingly being used to connect field devices, potentially exposing plant operating systems to risk [8]. Furthermore, due to the continual need to increase operational efficiency, large oil and gas corporations and drilling contractors are now relying on remote access due to costs involved or a shortage of personnel on board an offshore unit [9]. This has also contributed in making smart fields more vulnerable and appealing to cybercriminals. The increased sophistication of hackers contributes to the natural dread connected with cyberattacks. If one assault fails, the next one improves on the previous one and becomes more capable of penetrating or exploiting a flaw in the system. Unless offshore oil platforms choose to resort to entirely isolated networks, there is nowhere to ensure that a rig will be secure from cyber-terrorism. "We have embraced the goodness of technology and all that it brings us – efficiency and safety – but we haven't addressed the bad" [10]. There is a mismatch between the advantage of connection and the danger of connectivity on platforms. The oil and gas sector has been slow to recognize the hazards of inadequate cybersecurity on offshore oil platforms[10]. As a consequence, the days of a fictitious hacking threat are long gone, and we now live in a dangerous world. Hence, the industry is in desperate need of protection from these constant onslaughts. This study therefore aims at Combating Cyber Threats in Offshore Operations of Digital Oil Fields.

2. Related Work

© 2022 Afr. J. Comp. & ICT – All Rights Reserved
https://ajfcict.net
In their study, Progoulakis and Nikitas[11] looked into the notion of security risk assessment for offshore oil and gas installations, focusing on the instruments used to detect, assess, and reduce security threats. The paper's examination of statistics of reported security events for offshore oil and gas assets highlighted the need for security risk assessment. A number of security and risk assessment methodologies that are more suited to offshore oil and gas installations were given. The significance of integration of Process Safety Management, Security, and Risk Assessment was emphasized. A qualitative security risk management tool was demonstrated, emphasizing the need for a multidisciplinary approach to the mitigation of security risks.

Infosys [12] discussed the inherent limitations and security challenges that oil and gas organizations face, as well as the approaches that define the way forward for addressing the concerns. They also discussed the key factors that must be considered when defining and designing appropriate security roadmaps for long-term cybersecurity programs.

Roy et al [13] analysed and explained the principles of threat analysis from an "academic" perspective in their work. Other concepts such as impact assessment, desire, intent, capability, opportunity, and planning were discussed. There were descriptions of how the inherent threat and theoretical risk were assessed. A summary of the research imperatives for threat analysis was provided, as well as approaches to threat value stabilization based on neural networks and other mathematical techniques. Gelenbe et al. [15] presented and analysed a distributed and resilient attack detection and mitigation system for network settings in which communicating decision agents employed Graph Neural Networks to generate attack alarms. They also showed an attack mitigation system that employed a reinforcement Learning-driven Software Defined Network to handle alarms and Quality-of-Service measures to reroute important traffic away from vulnerable network pathways. The detection and rerouting schemes were demonstrated in the experiments.

Suganthi and Usha [16] offered a detailed overview of the taxonomy, as well as a description and arrangement of current research findings on intrusion detection systems in IoT devices. Thanks to this study, the researchers were able to uncover security problems resulting from information sharing technologies in the Internet of Things, as well as learn about numerous security threats and mitigation strategies.

Christopher et al. [17] proposed two methods for identifying botnet activity in consumer IoT devices and networks in their article. To begin, a detection model was built using Term Frequency-Inverse Document Frequency (tf-idf), which analyses network traffic for semantic structure and highlights semantic similarities between collected data and a known assault dataset. The detection of Mirai attack vectors in collected network data was determined using a similarity score. Second, a detection model based on a Recurrent Neural Network with Bidirectional Long Short-Term Memory was created using an unique Deep Learning application (BLSTM-RNN). The model was tested for accuracy and loss after detecting four attack vectors used by the Mirai botnet. Both techniques generate great outcomes, according to the article, and further research in this area seems promising.

MacKinnon et al. [18], looked at the differences between cyber terrorist and cybercriminal incidents, as well as the societal and technological changes that made such events more likely and devastating. The researchers then looked at three major components of cyber-terrorist attacks: cyber-attacks on physical systems, malware designed specifically for such attacks, and insider threats that enable or support such operations. They then looked at the countermeasures that organisations and individuals could use to address such threats, emphasising the human component of such systems by emphasising the importance of standards-based policies and protocols, good security hygiene, and system user training at all levels. Physical system upgrades and software tools for detecting and isolating cyber threats were also discussed. Finally, they discussed the expected continued growth of cyber terrorist acts, as well as the threat they pose to critical infrastructure and systems on which we are increasingly reliant, both socially and technologically.

3. Motivation and Open Problems

3.1 Offshore Platforms as Targets for Attacks

Despite changing opinions towards oil and a growing thirst for clean energy, offshore natural gas production has increased by more than 50 percent since 2000 [19]. Offshore production accounts for more than a quarter of today's oil and gas supply [20]. Offshore oil platforms, on the other hand, have always been a valuable target for both physical and cyberattacks [21]. Terrorists put a high value on these assets because of their role in producing energy and money for many nations, as well as the great destruction that an attack on them may do. If an offshore oil rig is attacked, the results can be severe. An act of terrorism carried out on a platform may disrupt a country's regular supply of electricity, deprive it of a crucial source of money, generate substantial and long-term environmental impact, and result in considerable loss of life [10].

Offshore oil platforms are also high-value targets for terrorists owing to their extreme susceptibility to physical and cyber assaults, as well as the incredible difficulty of defending them and the possible consequences of strikes [10]. Physical assaults on offshore platforms continue to be a hazard, but cyber-attacks are a tactic of attack that platforms are equally, if not more, susceptible to. Because of the linkage of the platform to the coast, drilling rigs that
were historically geographically separated are no longer isolated as the industry thinks.

3.2 Digitization Magnifies the Challenges
A complex ecosystem of computing, networking, and physical operational processes dispersed throughout the globe, in addition to the upstream sector's "critical infrastructure" designation, renders the industry especially susceptible to cyber-attacks. In other words, the industry has a vast attack surface and various assault vectors [5, diagram 1]. For example, a large oil and gas company employs half a million processors solely for reservoir simulation; generates, transmits, and stores petabytes of sensitive and competitive field data; and manages and shares thousands of drilling and production control systems across geographies, fields, vendors, service providers, and partners.

Security threats are also introduced by the technical setup of Industrial Control System (ICS). ICS software decisions are typically taken at the field or unit level rather than by corporate IT, resulting in solutions from a variety of solution providers, based on a variety of technologies, and with a variety of IT security requirements. The multi-decade life cycle of wells and ICS systems, as well as continuing asset sales and acquisitions, add to the complexity, making it difficult to account for, standardise, update, and retrofit these systems on a regular basis. For example, more than 1,350 oil and gas fields throughout the globe have been producing for more than 25 years, employing methods and equipment from diverse periods. [23]

In addition to the numerous benefits, increased digitization and interconnection of operations has increased cyber risks. Connected technology, in the form of digital oil fields or smart fields, has opened up an altogether new set of attack vectors for hackers by combining upstream activities in real time. Shell, for example, recently drilled a well in Vaca Muerta, Argentina, and controlled the drilling paseand pressure from a distant operations centre in Canada. [24]

What makes Internet of Things (IoT) technology both powerful and dangerous is its capacity to produce, transmit, collect, analyse, and act on data. Sensor technologies, wireless communications networks, and a range of analytical and automated tools allow the IoT phases, all of which are very susceptible to security breaches in outdated ICS systems and complicated upstream ecosystems. Protecting previously produced value while keeping ahead of future IoT adoption is a twofold cyber problem for the upstream oil and gas sector. [22]

Not all flaws in technology are the result of the technology itself. Internal actors wanting to undermine production, rivals looking to create brand harm, and external parties looking to shut down operations, such as activist organisations, are all potential sources of cyber risks. [5] It might also happen accidentally as a result of a lack of security awareness. Employees bringing infected portable media into the workplace, for example, might unwittingly expose systems to cyber-attacks due to a lack of security knowledge inside the firm. Furthermore, many operations staff just assume that their systems are unlikely to be attacked, thus they resist changing their routines and implementing new security policies. Another obsolete idea is that process failures are caused mostly by weather, human mistake, and equipment exhaustion, rather
than purposeful system manipulation by people who want to hurt others. [5]

The repercussions of a cyber breach, whether planned or inadvertent, may be severe, ranging from the compromise of sensitive data to system failure or shutdown. Reduced revenue, reputational damage, environmental disaster, legal penalties, and, in the worst-case scenario, death are all possible outcomes. [5]

5. Mitigating Cyber security Risk

Employees, regardless of size, are one of the most critical cybersecurity hazards in any firm. "Insiders carried out 60% of all assaults," according to a Harvard Business Review (HBR) study[14]. Three-quarters of the assaults were carried out with malevolent intent, while the other one-quarter were carried out by unintentional actors. [25]. Insiders who carry out malicious-intent assaults may be difficult to stop since the perpetrators generally know their way around the systems and can get beyond most of the perimeter protections, thanks to their valid access credentials. On the other hand, "inadvertent actor" assaults may be averted by training personnel about typical cybersecurity threats. Employees unknowingly participate as a vector of attack in many assaults because they do anything that compromises their user account credentials or workstation.

Employees that are taught about typical cybersecurity dangers may prevent many of these scenarios. Employees who are aware of phishing efforts and realise that certain security information is never sought in an email are less likely to hand up their credentials to a hacker. Employees are less likely to connect compromised devices to their network if a firm has a clear policy in place for utilising personal devices at work that they are aware of. Educating staff on certain email capabilities may help them prevent accidentally sending emails to the incorrect individuals. A staff with basic cybersecurity training is less likely to leak data or provide hackers unlimited access to their systems. Another important element to consider is the inclusion of a framework to improve cyber security in the energy industry. The National Institute Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity (CSF) helps firms evaluate their cybersecurity risks (threats, vulnerabilities, and consequences) and how to reduce those risks using tailored methodologies. The Framework's volunteer user base has expanded significantly throughout the nation and beyond the globe. It was created with the intention of benefiting private-sector owners and operators of essential infrastructure in the United States. The Framework integrates industry standards and best practices to help businesses manage cybersecurity risk. It creates a common language that allows personnel at all levels of a business – and at all points in the supply chain – to have a shared understanding of their cybersecurity concerns. In response to President Obama's executive order on defending privately-owned vital infrastructure, NIST published this study in 2014 as a consequence of the rising security, economic, public safety, and health risks posed by cyber security threats. The purpose is to improve the defence of critical infrastructure, which is crucial to the nation's security but is out of government control. "Regardless of an organization's size, threat exposure, or cybersecurity skill today, this strategy is required" [26].

The core functions of the NIST cyber security framework are: identify, protect, detect, react, and recover. [32, Fig 2]

Understanding the organization's aim and business requirements, as well as acquiring current landscape information to manage cybersecurity risk to systems, assets, data, and capabilities, are all part of the identification process. The identification function's operations are critical to the creation of a secure environment. Protect actions assist an organization in deterring cyber intrusion and harmful activities by establishing and implementing security policies to assure the availability and continuation of critical infrastructure services. Organizations should have a mechanism in place to detect and deter any intrusions, as there are possibilities that intrusions will continue to occur after controls and technology solutions have been implemented. It is nearly impossible to achieve a system with no points of entry. Respond is a critical step in which processes and activities within the team and organization are clearly identified, planned, and communicated. Recovery involves developing and implementing procedures for recovering from cyber incidents. To respond to all cyber incidents, these processes and procedures are developed and implemented. This allows the organization to reduce the impact of a cyber-security incident to a bare minimum. Because of the speed and intelligence of many of today's cyberattacks, cyber breaches may still occur; as a result, organizations should anticipate attacks and develop solutions to respond to them in real time.
6. Conclusions

In the oil and gas business, digitization of operational procedures has opened up new possibilities for increasing efficiency and lowering costs. However, this has exposed the company to a whole new set of cyber threats. For many years, the upstream sector, particularly offshore oil installations, has been a tempting target for terrorists. Cyber attackers have attacked the crude oil and natural gas (O&G) sectors as the industry embraces more networked technology, with assaults rising in frequency, complexity, and impact. Nonetheless, as hackers’ goals evolve - from cyberterrorism to industrial espionage to interrupting operations to collecting field data - firms increasingly depend on linked technology for day-to-day operations, dangers and stakes are constantly growing. As a result, the sector must be protected from these ongoing threats. Businesses can fight sophisticated hackers by anticipating assaults, reacting in real time, and securing assets depending on their worth. Despite all of the resources spent on strengthening cybersecurity, threat levels continue to climb faster than protection capabilities. With the exception of potentially unlawful acts such as hacking back, organisations must take all steps geared at predicting, detecting, redirecting, and isolating cyberattacks. That is, they must anticipate their encryption keys to be hacked, and that hackers would remain one step ahead of them when it comes to infecting their infrastructure with malware. Organizations must predict assaults before they happen, detect alarms in order to limit damage, and secure vital assets in a multi-tiered strategy.

References


