2021

# Perspectives on Cyber Security for Offshore Oil and Gas Assets

Iosif Progoulakis

Nikitas Nikitakos

Paul Rohmeyer

Barry Bunin

Dimitrios Dalaklis

*See next page for additional authors*

## Authors

Iosif Progoulakis, Nikitas Nikitakos, Paul Rohmeyer, Barry Bunin, Dimitrios Dalaklis, and Stavros Karamperidis

Journal of *Marine Science and Engineering*

MDPI

*Article*

# Perspectives on Cyber Security for Offshore Oil and Gas Assets

**Iosif Progoulakis [1,*], Nikitas Nikitakos [1], Paul Rohmeyer [2], Barry Bunin [3], Dimitrios Dalaklis [4] and Stavros Karamperidis [5]**

[1] Department of Shipping Trade and Transport, University of the Aegean, Korai 2a, GR82132 Chios, Greece; nnik@aegean.gr
[2] School of Business, Stevens Institute of Technology, 1 Castle Point on the Hudson, Hoboken, NJ 07030, USA; prohmeye@stevens.edu
[3] Maritime Security Center (MSC), Stevens Institute of Technology, 1 Castle Point on the Hudson, Hoboken, NJ 07030, USA; bbunin@stevens.edu
[4] Maritime Safety and Environmental Administration, World Maritime University, PO Box 500, SE-201 24 Malmö, Sweden; dd@wmu.se
[5] Department of International Shipping, Plymouth Business School, University of Plymouth, Logistics and Operations, Cookworthy Building, Drake Circus, Room 321, Plymouth PL4 8AA, UK; stavros.karamperidis@plymouth.ac.uk
* Correspondence: iprogoulakis@aegean.gr

**Abstract:** In an ever-evolving technological industry, the oil and gas sector is already moving forward through the adaptation of Industry 4.0 and the adaptation of advanced cyber technologies through Oil and Gas 4.0. As IT/OT (information technology/operational technology) systems are evolving technologically, so are the cyber security threats faced by the offshore oil and gas assets. This paper aims to raise the awareness of cyber security threats and the organizational and technical measures that need to be adopted by the oil and gas industry for remote and complex assets in the upstream sector. A comprehensive literature review covering the areas of new IT/OT systems integration and cyber security risk analysis and management is presented. The results of a survey on the subject of cyber security for offshore oil and gas assets are also presented, and they provide valuable insight into the current industry culture and the perception of cyber security concepts. The importance of organizational culture, personnel training and involvement, as well as corporate engagement and support in the subject of cyber security is highlighted.

**Keywords:** cyber security; offshore; oil and gas; critical infrastructure; survey



**Citation:** Progoulakis, I.; Nikitakos, N.; Rohmeyer, P.; Bunin, B.; Dalaklis, D.; Karamperidis, S. Perspectives on Cyber Security for Offshore Oil and Gas Assets. *J. Mar. Sci. Eng.* **2021**, *9*, 112. https://doi.org/10.3390/jmse9020112

Received: 7 December 2020
Accepted: 19 January 2021
Published: 22 January 2021



## 1. Introduction

The offshore oil and gas industry is characterized by its global presence and the dispersion of its upstream assets in all parts of the world. These assets, regardless of their type, i.e., drills ships, offshore production platforms, or FPSOs (floating production storage and offloading units), comprise multiple control systems, enabling safe and efficient exploration and production processes. These systems consist of industrial control systems (ICS) but combine the remoteness of their assets being offshore, thus sharing attributes with common maritime assets.

In an era of advanced digitalization of assets both in the maritime and oil and gas sectors, the implementation of digital twin technology, the use of cloud technology for digital storage, bandwidth, and communication of assets and processes and the IT (Information Technology) and OT (Operational Technology) systems that are on board offshore oil and assets, face numerous internal and external cyber security threats. Cyber attacks against oil and gas companies and the upstream domain have been going on for over 30 years [1]. More recently, it was reported that the percentage of ICS computers which had malicious objects blocked from accessing grew from 38% in H2, 2019 to 39.9% in H1, 2020 in the building automation industry, and from 36.3% to 37.8% in the oil and gas industry [2]. In

the maritime domain as reported in June 2020, an increase of cyber attacks by 400% was observed since February 2020 for maritime facilities and assets and their IT and OT systems and infrastructure [3]. The reported percentages of acknowledged cyber attacks indicate the imminent threat for offshore oil and gas assets.

This paper provides a perspective on cyber security of exploration and production assets in the offshore oil and gas domain coupled with industry data from a web survey of employees active in the industry. More specifically, the aim of this paper is to provide the following:

(a) An overview of available literature in the field of cyber security for offshore (upstream) oil and gas assets. As part of the literature review, any material exploring cyber security aspects involving the onshore assets and processes supporting the upstream sector will also be considered. The midstream and downstream sectors of the oil and gas industry are not covered in this paper as they are not part of the authors' research scope.
(b) An up-to-date view of the offshore oil and gas industry's perception of cyber security based on a survey of personnel active in the specific sector.

In general, the aim of this paper is to highlight the organizational, operational, and technical parameters that are influenced by cyber security threats and affect the cyber operations and integrity of the offshore oil and gas assets.

## 2. Digitalization and Cyber Integration in the Upstream Oil and Gas Sector

The introduction of data- and computer-driven technologies in the oil and gas sector is active and ongoing. The industry is embracing the Industry 4.0 era and its adaptation into "Oil and Gas 4.0" [4], as well as and the use of its digital tools and technologies, as the industry seeks their organizational and process integration. As outlined by Lu et al. [4], Industry 4.0 incorporates digital tools such as big data, the Industrial Internet of Things (IIoT), digital twin technology, wireless communication technologies, augmented reality (AR), and blockchain technology. Other technologies enabling the digital integration of the upstream oil and gas sector (both offshore and onshore) include machine learning, cloud computing, and artificial intelligence (AI). Oil and Gas 4.0 is applicable in the seismic exploration, intelligent oilfield, intelligent completion, and research and decision-making platforms [4,5].

The use and application of big data in the upstream oil and gas sector was reviewed in detail by Mohammadpoor and Torabi [6]. Its incorporation into Oil and Gas 4.0 and its applicability in the exploration and scouting, drilling, reservoir, and production engineering were outlined by Nguyen et al. [7]. The application of artificial intelligence in upstream drilling system design and operations was reviewed by Gharbi and Mansoori [8] and Bello et al. [9]. The digital twin concept was explained in detail by Elgonda LaGrange [10] and Holmås et al. [11]. The implementation of the Internet of Things (IoT) and its industrial adaptation in the IIoT was reviewed in detail by Thibaud et al. [12] in direct application to the oil and gas and energy sector.

In general, all abovementioned digital tools as part of Oil and Gas 4.0 are interconnected and interrelated in order to allow for the connectivity and interoperability of the information technology (IT) and operations technology (OT) systems within an oil and gas organization and in particular offshore oil and gas assets. The key components of this interoperability are the industrial control systems (ICS) and SCADA (supervisory control and data acquisition).

## 3. Literature Review on the Subject of Cyber Security in the Offshore Oil and Gas Domain

From a literature review, it is evident that the subject of cyber security for oil and gas assets is not widely studied, specifically for the offshore oil and gas domain. A lot of research has been conducted in the field of industrial cyber security as well as the maritime

domain, but the offshore oil and gas sector combines the attributes of both onshore facilities and maritime assets (vessels).

The publications that were identified consist of scientific journal articles and industry white papers, reports, directives, and standards that cover the following areas:

(a) Cyber security adversaries, threats, and vulnerabilities;
(b) Cyber systems integration as well as risk analysis and management;
(c) Industry and governmental initiatives.

These are outlined below so that the range of current research in the subject is realized.

### 3.1. Cyber Security Adversaries, Threats, and Vulnerabilities

In general, security threats initiated by adversaries against offshore oil and gas assets can be categorized as insider, external, or colluded (i.e., insiders working on behalf of external adversaries) [13]. These are translated to the following types of cyber adversaries:

(a) Cyber criminals: These comprise hackers, organized criminals, etc., seeking financial benefit through use of stolen digital information or manipulation of physical assets.
(b) State adversaries: They comprise hostile states seeking political advantage, espionage, destruction of digital assets, sabotage, etc.
(c) Insiders: They comprise disgruntled employees seeking personal benefit through targeted theft of digital information, destruction of digital assets, sabotage, etc., or negligent employees causing unwanted incidents [14].
(d) Cyber terrorists [15]: These are terrorist groups seeking sabotage or destruction of physical assets, and they exploit cyber and physical vulnerabilities for political or ideological reasons.
(e) Cyber activists: These comprise hacktivists and activist groups causing sabotage to cyber infrastructure through targeted cyber attacks for political or ideological purposes.

Soares and Souza [16], Hacquebord and Pernet [17], and Ginter [18] have validated the above adversaries by providing examples of real-world threat and attack scenarios. The Lawrence Livermore National Laboratory (LLNL) [19], Hacquebord and Pernet [17], and Dragos Inc. [20] have provided a very comprehensive list of these adversaries, such as Xenotime, Magnallium (also known as APT 33), Chrysene, Hexane, Dymalloya, and others, all targeting oil and gas corporations and assets through strategic and opportunistic attacks. Cyber attack scenarios and consequences that have been noted include the following:

- Remote manipulation of offshore platform OT systems, causing failure of operational and safety systems [15,20];
- Remote data hijacking and manipulation for targeted physical attacks to maritime and offshore oil and gas assets [16];
- Sabotage of IT and OT systems by an employee for personal benefit [15];
- A cyber attack scenario on an offshore natural gas asset by the altering of parameters in the gas hydrate system [21];
- Compromise of a third-party and original equipment manufacturer (OEM) [20], aiming at the cyber espionage and hacking of IT/OT systems, and infiltrating internal cyber security barriers of offshore oil and gas assets and organizations;
- Cyber attack against shore-based electric power generation and supply entity of shore-to-offshore power distribution, aiming at the disruption of upstream and midstream oil and gas asset operations [20].

The combinations of attack scenarios and methodologies as described above and in detail by Stergiopoulos et al. [22] and Moreno et al. [23] are numerous. In general, it can be observed that cyber security threats leading to cyber attack incidents can affect the offshore oil and gas asset itself along with its IT/OT systems (pumps, remote terminal units, PLCs, sensors, etc.), its shore-to-offshore infrastructure (pipelines, power and communication connections), its onshore infrastructure and corporate data centers, supply logistics, IT control centers, etc.

For the corporate and onshore infrastructure supporting offshore oil and gas assets, the adversaries remain the same, but the types of cyber attacks and threats relate more to the financial sector. Rohmeyer and Bayuk [24] pointed to the theft of funds or data and operational disruptions as major threats for financial organizations, which correlates to recent cyber attacks in oil and gas companies. The Saudi Aramco cyber incident affecting over 30,000 corporate computer systems and causing major supply and operational halting [25] confirms the disruption threat to the oil and gas sector, its onshore infrastructure, and its offshore assets. Data leaks and their subsequent financial impact in oil and gas contract bidding [26] also confirm the impact from data theft or leakage and industrial espionage as well as the indirect loss of funds. Even though the majority of cyber attack incidents in the oil and gas domain remain unpublished, the above are realistic examples of the exploitation of asset vulnerabilities.

In accepting upstream oil and gas sector assets as critical infrastructure, it is understood that they consist of a complex grid of computation, networking, and physical operational processes [27], involving assets and systems positioned in multiple remote locations and at a great distance between them. This makes the upstream oil and gas sector vulnerable against security threats in the physical and cyber domain. Assuming that cyber threats are defined as computer or computer network hazards (Lewis 2020), the threats for critical infrastructure such as offshore oil and gas assets can vary from malicious software and malware to phishing email exploits [28]. Hacquebord and Pernet [17] as well as Folga et al. and their Argonne National Laboratory Report [29] and NTT Security [30] provided a detailed list of such malign threats:

- Infrastructure sabotage: This refers to the use of malware or malicious software for the manipulation and damage of IT/OT infrastructure, as well as the alteration of data and equipment operating parameters, all leading to the malfunction and/or damage/destruction of assets, systems, etc. One example is the Stuxnet virus used in the attacks against the Iranian uranium-enriching facilities' OT systems, which also affect IT systems from the U.S. oil and gas company Chevron [31]. Another example is the targeted cyber espionage campaign against gas pipeline companies to gather data for sabotage operations [29].
- Data leaks: These are caused by the unsafe handling or storage of data through web or file servers as well as through targeted hacking attacks.
- Insider malicious cyber incidents: These comprise insider-led destruction or alteration of data, theft of intellectual property, and data leakage.
- Attacks on webmail and corporate VPN servers: This is achieved through DNS (Domain Name Server) hijacking or targeted phishing attacks.
- DNS (domain name server) hijacking: This involves the modification of corporate domain name servers for the theft of corporate credentials, email communication interception, access to internal and VPN networks, etc.
- Espionage and data theft: This involves intrusion into corporate IT systems for the theft of data and/or monitoring of financial transactions, corporate data processing, etc. This threat scenario was confirmed by the ENISA report ETL 2020 on the cyber espionage threat landscape [32].
- External emails: These are data leaks caused by the use of external email communication through corporate or personal computer systems, whereby the unsafe storage or transmission of data becomes a risk.
- Malware: This comprise adware or spam, trojans, bots (used also for distributed denial-of-service (DDoS) [28], ransomware, rootkit, spyware, viruses, worms [28] that are used to gain access to IT/OT systems, to remotely intervene, control, or monitor processes, to access data, etc.

From the types of cyber incidents, threats, and adversaries described, it is evident that the vulnerabilities, whether already existing or created, derive from the necessary data transfer between the different functions of an oil and gas asset and organization. Data transfer between field operations and IT/OT systems to corporate IT systems or data

centers allows for multiple security breach paths and vulnerabilities [33]. The company DNV GL [34] has identified the following most prominent vulnerabilities for offshores oil and gas assets with regard to their cyber security:

(a) Lack of cyber security awareness and training of employees
(b) Remote work during operations and maintenance
(c) Using commercial type IT products with known vulnerabilities in the production environment
(d) An inadequate cyber security culture among vendors, suppliers and contractors
(e) Insufficient separation and segmentation of data networks
(f) The use of mobile devices and storage units including smartphones
(g) Data networks between on- and offshore facilities
(h) Insufficient physical security of data rooms, cabinets, etc.
(i) Vulnerable software
(j) Outdated and ageing control systems in facilities

All the above are in full correlation to the real incidents described previously, and they outline the complexity of IT and OT systems and processes as well as a high reliance on electronic, networked, and remote systems and subsystems resulting in a large attack surface and many attack vectors [27].

### 3.2. Cyber Systems Integration and Risk Analysis and Management

In the area of systems integration and cyber security risk management for IT/OT infrastructure of offshore oil and gas assets, a number of journal publications were reviewed. More specifically, Yang, Cao, and Li [35] carried out an analysis of the structure and safety deficiencies of oil and gas SCADA (supervisor control and data acquisition) network, aiming to evaluate the limitations of traditional evaluation methods. They proposed a new network security risk evaluation method of oil and gas SCADA, through a combination of factor state space and the fuzzy comprehensive evaluation method. Vieira, Houmb, and Insua [36] proposed a graphical model for cyber security risk assessment based on an adversarial risk analysis for the mitigation of cyber security challenges. They also presented an example of application of the graphical model for an offshore drilling rig, indicating the use of standard business language based on decisions, risks, and value, but on a more formal and comprehensive risks analysis method. Prasad and Avadhani [37] presented the design and analysis of attack trees implemented in offshore oil and gas process complex SCADA systems. Their aim was to identify system vulnerabilities and expose methodologies used by attackers when they attempt to take control of the SCADA systems in order to affect hydrocarbons production. Refsdal, Solhaug, and Stølen [38] demonstrated the application of a security risk analysis methodology for the tackling of threat scenarios on a case involving the introduction of new decision support software technology for the handling of work permit applications in the oil and gas domain. Their methodology is to calculate the frequency rather than the probability of threat scenarios, and it focuses on the implementation of system as well as the operational and organizational changes at a corporate and field level in oil and gas assets. Marcin and Emilian [39] proposed an integrated risk analysis and assessment methodology compatible with industrial hazard and risk identifications methods such as HAZOP (hazard and operability), LOPA (layer of protection analysis), and SVA (security vulnerability analysis). Their methodology addresses risk mitigation by considering the safety and security requirements as per IEC 61508, IEC 61511, and IEC 62443 standards and is applied to oil port installations and related critical infrastructure. Kosmowski and Gołębiewski [40] proposed an approach for the proactive reliability, functional safety, and cyber security management and predictive risk analysis of oil ports, hazardous plants, and critical infrastructure by considering the security levels outlined by the ISPS Code. Their approach was based on the analysis of relevant hazards/threats and evaluation of related risks, while considering also the perspectives of underwriters and insurance companies. The implementation of innovative technologies such as Industry 4.0 and the convergence of advanced OT/IT (operational technology/information technology)

systems were also considered. McEvoy and Wolthusen [41] proposed the use of causal Bayesian networks to analyze probable attack strategies on a managed pressure drilling (MPD) system that was on board an offshore oil and gas asset. Their work can assist oil and gas corporations to realize cyber security risks and recover from cyber attack incidents.

The area of cyber systems integration and their relation to cyber security incidents and vulnerabilities has been covered by a number of journal articles. From these, Fataliyev and Mehdiyev [42] investigated the use of Internet of Things in the oil and gas sector and specifically in the Azerbaijani oil company SOCAR from the context of cyber physical systems. They proposed new approaches for the mitigation of technical problems in integrated smart sensors, the Internet of Things, wireless networks, and cloud technologies for cyber physical systems. Aalsalem et al. [43] described the application of wireless sensor networks (WSNs) in the upstream oil and gas sector; they highlighted the cyber security requirements to ensure the safety and security integrity of infrastructure and to thwart cyber attacks, network and system failures, and operational disruptions. Similarly, Radmand et al. [44] outlined the various types of cyber attacks in wireless sensor networks (WSNs) for oil and gas assets, and they acknowledged that system vulnerabilities are not adequately investigated in the industry. Their proposal is to utilize WSNs only for system redundancy, not allocating them in critical functions, and to consider contingency plans for their potential interruption or malfunction. Sveen et al. [45] developed a model of integrated operations for the North Sea wells, targeting the remote operation of offshore oil and gas assets for the increase of production levels, the reduction of operational costs, and the extension of lifespan. Their work involved the implementation of new technologies in an organizational, technical, and operational level and considered the improvement of system, infrastructure, cultural, and operational security risk management and vulnerability assessment. Similarly, Rydzak et al. [46] used a generic risk matrix and explored the allocation of resources in infrastructure and systems in offshore oil and gas assets, aiming at their resiliency built up and reinforcement against cyber threats. Spandonidis and Giordamlis [47] also acknowledged that cyber security as a factor affects the use of 5G mobile networks and Industrial Internet of Things (IIoT) for data-centric operations. Finally, Erkoyuncu et al. [48] investigated the identification and quantification of IT/OT systems' software obsolescence in the oil and gas sector. Their developed tools and methodology that evaluated obsolescence impact, risk exposure, capital and operating expenditure, and resolution implementation, aiming at the reinforcement of infrastructure from exposed system vulnerabilities and the elimination of safety and cyber security breaches.

### *3.3. Industry and Governmental Initiatives*

Various governmental entities around the world, industry organizations, and the oil and gas industry have developed and continued to develop a number of legislations, directives, standards, and guidelines to proactively and reactively deal with the current and emerging cyber security threats. A description of such indicative documents specifically relevant to or created for the offshore oil and gas domain is given below, without being a conclusive list.

Regarding industry standards, directives, and guidelines, the U.S. National Institute of Standards and Technology (NIST) Cyber Security Framework is the most commonly used and widely applicable in the USA and elsewhere. It consists of a framework of standards that capture the operational and technical cyber security requirements of industrial, maritime and offshore oil and gas assets. It consists of five functions: (1) the identification of cyber security risks to systems, assets, data, and operations; (2) the protection of assets by the implementation of safeguards; (3) the detection of cyber security incidents; (4) the response to cyber security events; and (5) the recovery from cyber security breaches. The NIST Cyber Security Framework is supplemented by NIST Special Publications 800-30, 800-37, and 800-82, which cover cyber security risk assessment and management for industrial control systems (ICS). The NIST Cyber Security Framework is also applied by the standard ASTM F3286-17 (2017), applicable to maritime assets and critical infrastructure.

Internationally, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have developed and issued a number of standards applicable to cyber security, such as ISO/IEC 27001, IEC-62443-4-2, IEC 62443-3-3, ISO/IEC 21827, ISO/IEC 15408-1, ISO/IEC 18045, and ISO/IEC 27032. These cover risk assessment and management, as well as the mitigation of vulnerabilities in Industrial Automation and Control Systems (IACS), and they describe the Systems Security Engineering Capability Maturity Model® (SSE-CMM®).

The American Petroleum Institute (API) has created Recommended Practices (RP), API RP 70 (2003) and API RP 70I (2003), which are related to the security assessment of offshore oil and gas assets, and these are applied both in the U.S. and internationally. API has also published Standard (STD) 780, outlining a Security Risk Assessment (SRA) methodology for the petroleum and petrochemical industry. The abovementioned API recommended practices and standards are generic in the planning against or the mitigation of physical security threats but can also apply to cyber security threats as they would involve IT/OT systems that are critical for the integrity and safety of assets. For the technically related subject of cyber security, API Standard 1164 was published to cover the security of SCADA systems for pipeline assets, covering both the offshore and onshore environments.

In the sector of industry organizations, the International Maritime Organization (IMO) released Resolution MSC.428(98) and IMO Guidance MSC-FAL.1/Circ.3 in 2017. Both address the implementation of maritime risk management in vessels' safety management systems (SMSs) in accordance with the ISM (International Safety Management) Code objectives and requirements, complementing the IMO ISPS (International Ship and Port Facility Security) code. Both IMO documents apply primarily to maritime assets but do not exclude maritime oil and gas assets such as drill-ships, FPSOs (floating production storage and offloading units), and FSRUs (floating storage regasification units). Resolution MSC.428(98) is also adopted by standard ASTM F3449-20 and is applicable to maritime assets. Similarly, the International Association of Drilling Contractors (IADC) has issued guideline documents "Assessing and Managing Cybersecurity Risks to Drilling Assets (2015)" and "Guidelines for Baseline Cybersecurity for Drilling Assets (2018)". They deal with the assessment and management of cyber security risks and outline existing international and regional standards, including the NIST Cybersecurity Framework and ISO/IEC 21827.

In the governmental sector in the U.S., the U.S. Department of Homeland Security (DHS) and the Department of Energy (DoE) (2014) developed the Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2) in order to assist the industry to evaluate and improve their cyber security infrastructure and capacity, implementing the National Institute of Standards and Technology (NIST) Cyber Security Framework. In the maritime domain, the U.S. Coast Guard (2020) has issued Navigation and Vessel Inspection Circular (NVIC) 01-20, titled "Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities", providing guidance to facilities to assess, document, and address computer system and network cyber vulnerabilities in their assets. NVIC 01-20 covers maritime assets and facilities in the outer continental shelf and offshore operations, and it covers offshore oil and gas assets operating under U.S. MTSA provisions. The U.S. Congress (2020) also issued Bill S. 4023 "Enhancing Maritime Cybersecurity Act of 2020", which delegates the implementation of cyber security strategies and measures to the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the Maritime Administration (MARAD).

In the European Union, cyber security for the oil and gas sector is addressed from the spectrum of critical infrastructure protection. European Union Directives 2008/114/EC and 2013/30/EU tackle the critical infrastructure element in general and the safety for offshore oil and gas assets without explicitly covering cyber security. In particular, 2016/1148/EU addresses the cyber security of IT networks without specifically specifying the infrastructure, systems, or assets related to the upstream oil and gas sector. It should also be noted that a revision to 2016/1148/EU was proposed on December 16, 2020. The European

Union's cyber security strategy JOIN/2013/01 was also developed to strategically implement mitigation technologies and policies and to raise cyber resilience and security levels. As per directive 2019/881/EU, also known as the EU Cybersecurity Act, cyber security is handled by the European Union Agency for Network and Information Security (ENISA), which develops, recommends, and implements policies, standards, directives, and technologies to mitigate cyber security threats across the European Union member states. The ENISA Report of 2016 [49] assessed the oil and gas sector without providing any specific recommendations.

Finally, in the Asian region, the Maritime and Port Authority of Singapore published Shipping Circular No.15 on Maritime Cyber Risk Management, which enforces the requirements of IMO Resolution MSC.428(98) and IMO MSC-FAL.1/Circ.3.

In the sector of maritime classification societies, the American Bureau of Shipping (ABS) has issued five guidance documents that apply to operators, owners, as well as vessel construction and integration companies for offshore and maritime assets. These provide best practices for the implementation of cyber security measures in the operational and technical level and the application of mitigation measures for information technology (IT) and operational technology (OT) systems for maritime and offshore assets ensuring data integrity.

DNV GL in turn has issued recommended practices DNVGL-RP-G108 (2017), DNVGL-RP-0496 (2016), and DNVGL-CP-0231 (2018). DNVGL-RP-G108 provides a guideline for the application of the IEC 62443 series of standards in the oil and gas industry in general. DNVGL-RP-0496 provides guidance to asset owners and operators on enhanced cyber security practices and resilience management for ships and mobile offshore units. DNV-CP-0231 describes the certification process for increased cyber security for systems and components to be installed on board vessels as well as offshore installations.

Lloyd's Register (LR) developed three guidance notes that cover maritime assets and the deployment of IT and OT, autonomous ships, and the type approval of cyber-enabled vessel systems components as well as the LR Cybersecurity Framework (CSF) for the marine and offshore sector adopting the IMO regulations.

The Japan Maritime Association (Class NK) has issued guideline documents "Guidelines for designing Cyber Security Onboard Ships" (Class NK 2020) and "Cyber Security Management Systems for Ships" (Class NK 2019). These apply to maritime vessels and column-stabilized drilling units, and they describe the implementation of controls against cyber threats for IT and OT systems and the implementation, maintenance, and improvement of cyber security management systems for companies and maritime assets aiming at safe navigation.

The governmental and industry initiatives described in this section are summarized in Table 1 and are in agreement with the industry regulations and standards outlined by reports from the Lawrence Livermore National Laboratory (LLNL) [19], Holcomb from LEIDOS [49], and the Oil and Natural Gas Subsector Coordinating Council (ONG SCC) and Natural Gas Council (NGC) [50,51].

**Table 1.** Summary of governmental and industry initiatives related to cyber security.

| Category | Originator | Title |
|---|---|---|
| Standards | NIST | NIST Special Publications 800-30, 800-37, 800-82 |
| | ASTM | ASTM F3286-17, ASTM F3449-20 |
| | ISO/IEC | ISO/IEC 27001, IEC-62443-4-2, IEC 62443-3-3, ISO/IEC 21827, ISO/IEC 15408-1, ISO/IEC 18045, and ISO/IEC 27032 |
| | API | API RP 70, API RP 70I, API RP 780, API Standard 1164 |
| Industry organizations | IMO | IMO Resolution MSC.428(98), IMO Guidance MSC-FAL.1/Circ.3 |
| | IADC | IADC guideline: "Assessing and Managing Cybersecurity Risks to Drilling Assets (2015)" IADC guideline: "Guidelines for Baseline Cybersecurity for Drilling Assets (2018)" |
| Government | DHS and DoE | Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2) |
| | USCG | NVIC 01-20 |
| | U.S. Congress | Bill S. 4023 "Enhancing Maritime Cybersecurity Act of 2020" |
| | European Union | 2008/114/EC, 2013/30/EU, 2016/1148/EU, 2019/881/EU, EU Cybersecurity strategy JOIN/2013/01, ENISA report 2016 |
| | MPA Singapore | Shipping Circular No. 15 (2020) |
| Maritime classification societies | ABS | ABS "Guidance Notes on the Application of Cybersecurity Principles to Marine and Offshore Operations—ABS CyberSafety Vol. 1", September 2016 ABS "Guide for Cybersecurity Implementation for the Marine and Offshore Industries—ABS CyberSafety Vol. 2", June 2018 (revised) ABS "Guidance Notes on Data Integrity for Marine and Offshore Operations—ABS CyberSafety Vo. 3", September 2016 ABS "Guide for Software Systems Verification—ABS CyberSafety Vol. 4", September 2016 ABS "Guidance Notes on Software Provider Conformity Program—ABS CyberSafety Vol. 5", September 2016 |
| | DNV GL | DNVGL-RP-G108 (2017), DNVGL-RP-G 496 (2016), DNVGL-CP-0231 (2018) |
| | Lloyd's Register | Lloyd's Register Guidance Note: Cyber-enabled ships—Deploying information and communications technology in shipping—Lloyd's Register's approach to assurance, 2016. Lloyd's Register Guidance Note: Cyber-enabled ships—ShipRight procedure—autonomous ships, 2016. Lloyd's Register Guidance Note: Cyber-enabled ships—Type Approval of Cyber Enabled Systems Components, 2016. |
| | Class NK | Class NK, "Guidelines for Designing Cyber Security Onboard Ships", 2nd Ed., July 2020. Class NK, "Cyber Security Management Systems for Ships", 1st Ed., April 2019. |

### *3.4. COVID-19 and Its Cyber Security Implications in the Offshore Oil and Gas Domain*

In extreme situations like the COVID-19 pandemic, the oil and gas industry faced the same operational difficulties as also faced by many other industry sectors. Both the personnel working on shore supporting offshore operations and the offshore workers were equally vulnerable to health issues. Especially for the personnel working offshore, the COVID-19 situation adversely affected the rotation of personnel's shifts, prolonged their time offshore, and prevented shore-to-rig transportation, leading to the reduction or alteration of maintenance activities in OT and IT systems [52]. This created further vulnerabilities to OT and IT systems as software security updates were not frequent or not carried out as scheduled. In addition, the remote working for many oil and gas professionals on shore resulted in pushing the cyber integration of the industry further and increasing the vulnerability of systems and organizational functions since cyber security barriers had to be adapted from the office/industrial plant to the home environment. People working from their home and supporting the offshore oil and gas industry were

vulnerable to increased cyber risks from phishing attacks and cyber criminals [53]. It is evident that all existing mitigation measures for cyber attacks remain valid for these difficult times where company workers have to use their own common sense for cyber safety rather than rely on corporate firewalls and IT support. As threats will continue to evolve, so should the IT and OT infrastructure for oil and gas companies. This could be achieved by identifying new cyber protection barriers as well as reshaping their IT/OT infrastructure and move from the decentralized information databases (device-led IT) to the more centralized infrastructure (server-led IT) where vulnerabilities from personnel standalone workstations can be reduced by relying on information transfer through virtual or hosted desktops utilizing on-premises servers or the cloud [53]. The offshore oil and gas industry has to build resiliency within its organization as well as its operational and technical infrastructure in order to mitigate cyber security risks in the case of extreme scenarios such as the COVID-19 pandemic.

## 4. Industry-Wide Survey on Cyber Security for Offshore Oil and Gas Assets

### *4.1. Survey Methodology and Objectives*

In order to validate the state of cyber security for offshore oil and gas assets, a survey was carried out between February and July 2020 where input from professionals who engaged actively in the offshore oil and gas industry was requested. Google Forms was used for creating the survey questionnaire as it was found to be more easily distributed electronically and could also guarantee the anonymity of the participants. Distribution of the survey was done using direct communication to individuals through the LinkedIn professional social media platform as well as through direct email communication to known industry contacts. The professionals contacted included both "white-collar" and "blue-collar" employees. The pool of individuals included engineers, technicians, third-party consultants, superintendents, rig managers, academics, and corporate executives involved directly or indirectly in the technical, operational, or management side of offshore oil and gas assets. Individuals employed in government agencies and the military were also contacted as their work involved the direct or indirect protection of critical infrastructure such as upstream oil and gas assets. In total, 350 individuals were contacted from companies, prime contractors, subcontractors, third-party service or consultancy providers and government and military entities from all over the world. A total of 66 (18.8%) anonymous responses were gathered and used to analyze data for this publication. It should be highlighted that from those contacted, a large number did not respond to the survey due to the sensitivity of the cyber security subject or lack of knowledge in the field. In addition, from the communication to the survey participants, a large percentage of participants were reluctant to respond to the survey request and email communication due to confidentiality and cyber security concerns. Contact with industry organizations such IADC (International Association of Drilling Contractors) and IOGP (International Association of Oil and Gas Producers) was attempted for wider distribution of the survey but with no success.

The survey questionnaire was structured in such a way that generic information could be gathered regarding industry compliance (standards) for cyber security and risk analysis, the perception of cyber security threats, vulnerabilities, mitigation barriers and incident consequences in assets and the organizational and personnel delegation of cyber security duties. More specifically, the survey questionnaire was structured into eight sections. Part 1 gathered generic information on the background of the survey participants (company type, being an asset owner, contractor, consultant, etc.), as well as the location of the upstream assets operated. Part 2 collected information on the cyber security training and delegation of duties for company personnel and contractors involved in the operation or maintenance of IT and OT assets. Part 3 enquired about the information technology (IT) initiatives implemented by companies to optimize cyber security and the constraints they faced at a corporate and field level. Part 4 looked into the perception of cyber security vulnerabilities, threat scenarios and cyber attack consequences for offshore oil and gas assets. Part 5 examined the operational integration of cyber security onboard offshore oil and gas assets

in relation to the permit-to-work system, the monitoring of key performance indicators (KPIs), and the built-in system and asset resiliency. Part 6 explored the organizational and field asset compliance to industry standards and governmental directives on cyber and security risk assessment. Part 7 explored the relation of operational process safety and cyber security measures. Part 8 explored the industry's reliance on external support for cyber security services and the adequacy of existing legislative and directives' cyber security framework. The process that was followed to implement the design, distribution, and processing of the survey questionnaire can be seen in Figure 1.

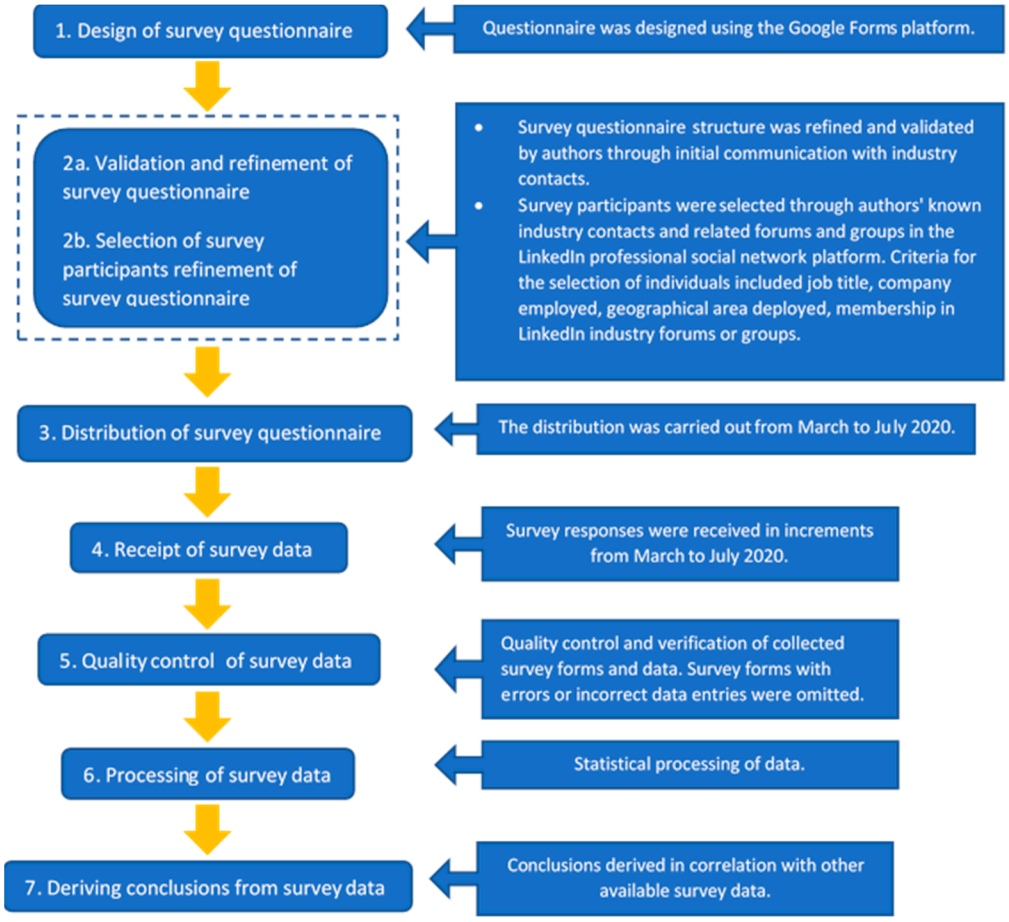


**Figure 1.** Survey process followed.

### *4.2. Survey Results and Analysis*

From the participants of the survey, a 44% represented offshore oil and gas asset owners, meaning the personnel working in corporations who own such assets. A total of 29% represented contractors occupied on offshore oil and gas assets, from which 18% represented contractor companies who operate assets, 3% provides the personnel to operate assets, and 8% refers to companies providing technical contracted tasks. A total of 23% represented third-party consultancy companies, from which 18% referred to companies providing some sort of consultancy services and 5% referred to offshore oil and gas asset classification or registry organizations. A combined 5% referred also to OEM and academic institution participants with knowledge of or involvement in the offshore oil and gas operations.

From the participants' responses, it was observed that they represented offshore oil and gas assets, from which 40% were from multiple geographic regions around the world. 29% were located in Europe, 13% in the Asia Pacific region, 6% in North America, 4% in the CIS (Commonwealth of Independent States) region representing countries of the post-Soviet era. In addition, 3% of the assets were located in the Middle East region, 2% in Central

and South America, 2% in the African continent, and 1% in the Eastern Mediterranean region. The wide dispersion of assets is evident, and it provides a representative sample of world-deployed and operated assets and personnel. The described results regarding the survey participants and representative assets are presented in Figures 2 and 3.

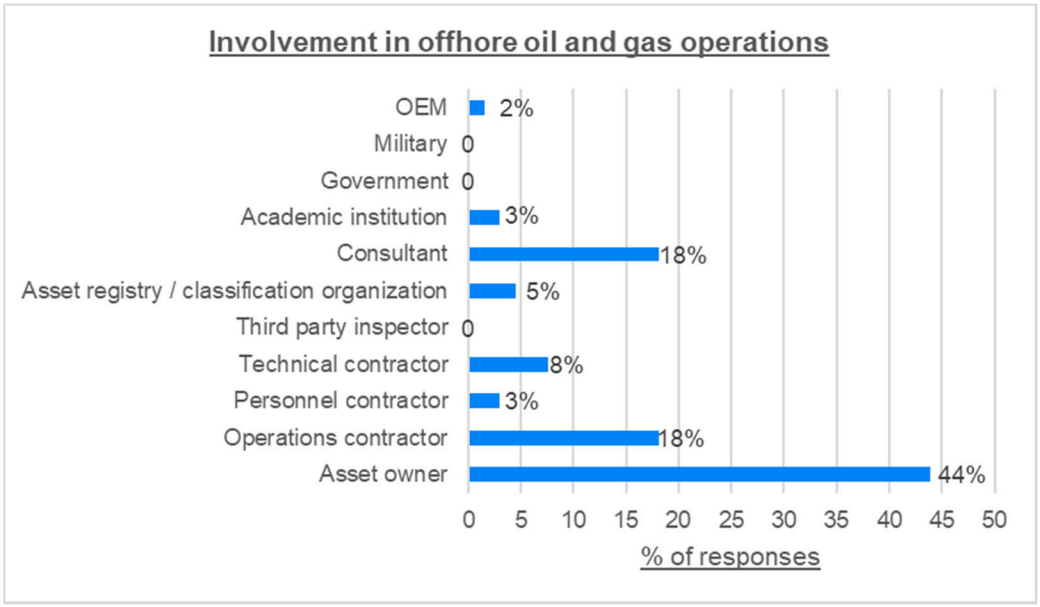


**Figure 2.** Survey participants' involvement in offshore oil and gas operations.

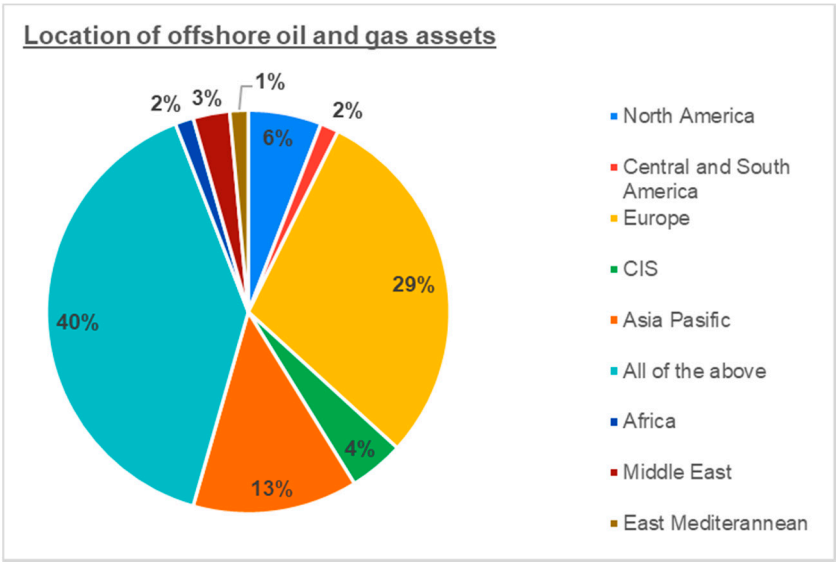


**Figure 3.** Location of offshore oil and gas assets.

In regard to personnel involvement and training on cyber security, 64% of participants responded that oil and gas companies' employees receive training for cyber security. For contractors' personnel, this percentage is at 50%, whereas 38% responded that contractors are involved in onboard cyber security duties on the assets; 53% responded that a designated and dedicated person onboard the offshore oil and gas assets is responsible for cyber security duties, and 86% confirmed that oil and gas companies have a dedicated department or entity within their organization that is responsible for cyber security duties. The above are depicted in Figures 4–6.

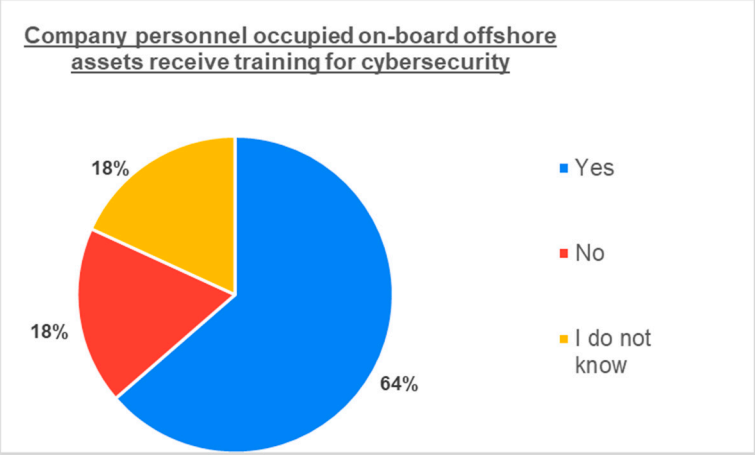


**Figure 4.** Company personnel occupied on board offshore assets, receiving training for cyber security.

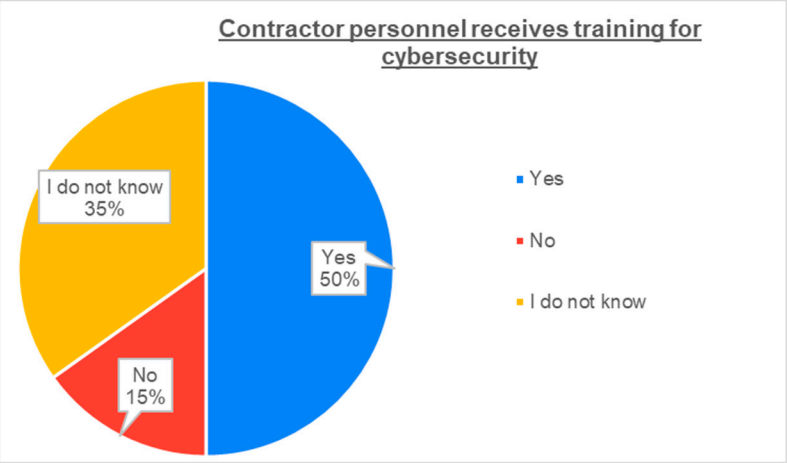


**Figure 5.** Contractor personnel receiving training for cyber security.

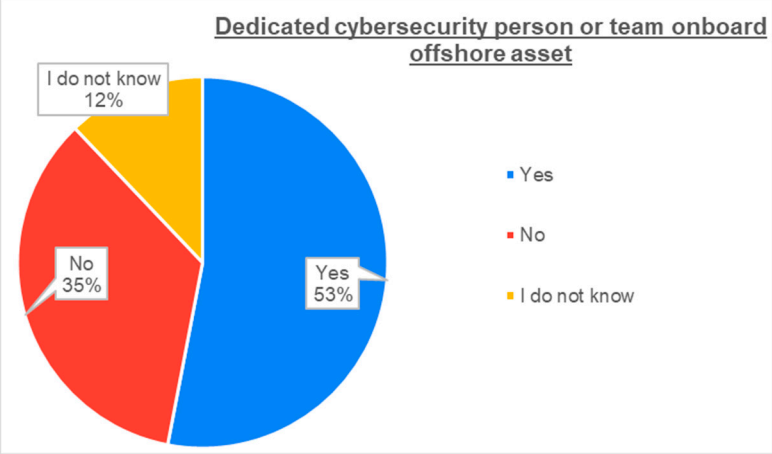


**Figure 6.** Existence of a dedicated cyber security person or team on board offshore oil and gas assets.

Regarding the enquiry about the information technology (IT) initiatives implemented by companies to optimize cyber security, a number of options were available for responses from which the most important were the use of firewalls (95%), corporate policies on the use of IT procedures and system passwords (94%), and the use of antivirus software on IT systems (91%). For the restrictions faced by corporate organizations in the implementation and deployment of cyber security measures, 48% of participants declared the lack of

understanding of the cyber security threats and consequences, 41% the budget restrictions, and 35% the corporate culture on cyber security. The results of these survey queries are shown in Figures 7 and 8.

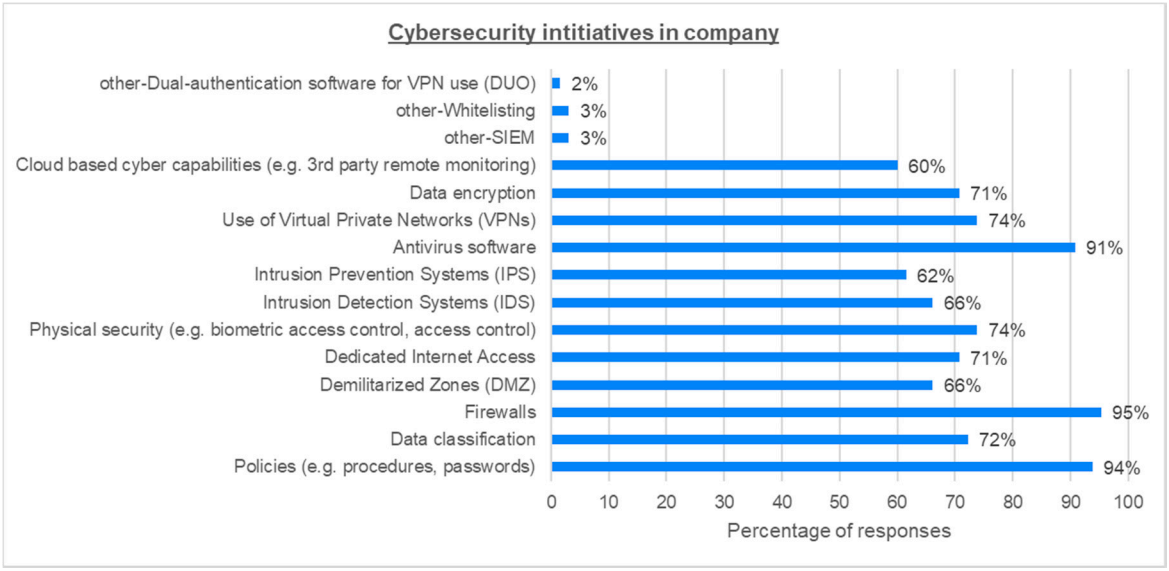


**Figure 7.** IT (information technology) cyber security initiatives implemented by companies.

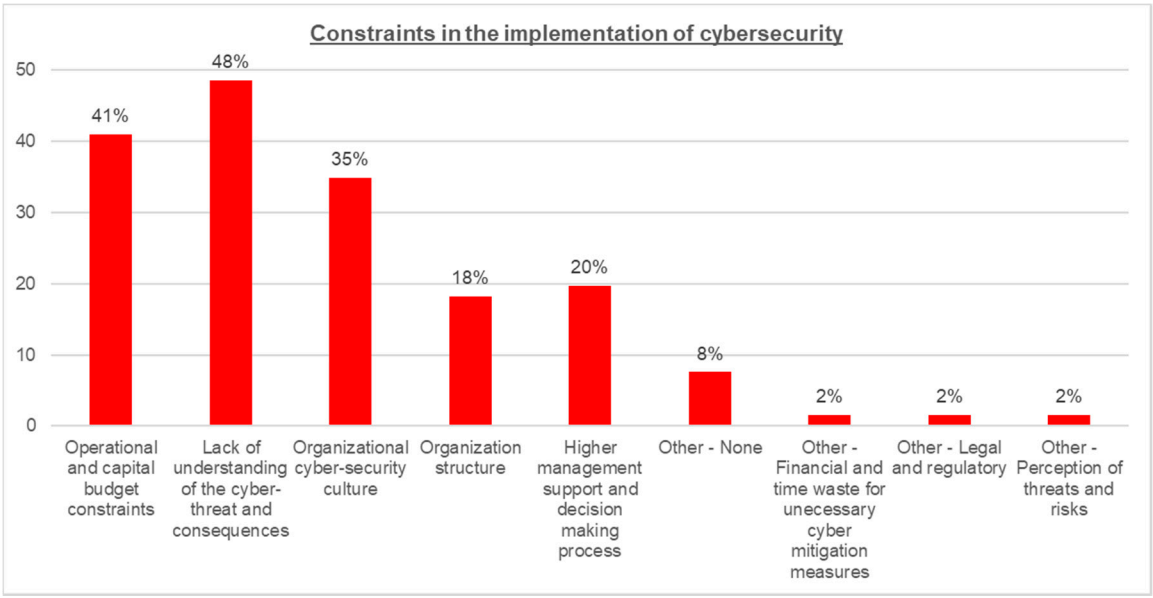


**Figure 8.** Constraints in the implementation of cyber security.

For the exploration of cyber security vulnerabilities for the offshore oil and gas domain, the participants identified the following: portable USB devices (67%), low employee awareness (59%), outdated control and monitoring system architecture (53%), number of devices with access to critical data (41%), Wi-Fi network (39%), and cloud monitoring and control infrastructure (24%). Similarly, for the OT and IT vulnerabilities that can lead to cyber security incidents, the company personnel awareness and training was identified by 71% of participants. Organizational cyber and physical security culture was identified by 62% of participants, followed at 61% by the legacy systems in back-up/secondary asset systems, improper integration of new IT systems into existing infrastructure at 56%, and

the lack of upstream process knowledge from IT personnel at 35%. These statistics are presented in Figure 9.

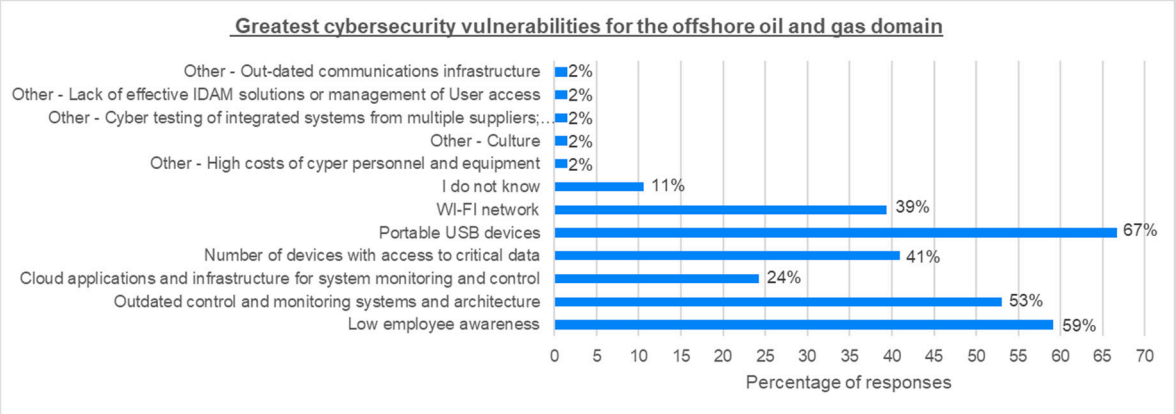


**Figure 9.** Cyber security vulnerabilities for the offshore oil and gas domain.

For the most probable types of cyber security threats faced by offshore oil and gas assets, as depicted in Figure 10, 67% of the participants identified email hacks, followed by ransomware (56%), phishing (55%), malicious insider threats (45%), remote control of systems (44%), data breaches (42%), cyber espionage (39%), and denial of service (38%). Some of these threats can actually be translated into cyber breaches on IT/OT infrastructure and its users and systems. Interestingly, a further analysis of the survey in Figure 11 indicates that 73% of the participants acknowledge a deliberate malicious act by an insider employee or contractor as a probable cyber threat scenario. This percentage reflects the survey participants' opinion on a malicious insider as a standalone threat in comparison to Figure 10 where it is listed among the other threats. In regard to the perceived vulnerabilities of the systems, components, or assemblies on board an offshore oil and gas asset, personnel workstations, communication systems, and process control stations are rated most highly by survey participants. Finally, the imminent threat of unmanned platforms or drones such as UAVs (Unmanned Aerial Vehicles), USVs (Unmanned Surface Vehicles) and UUVs (Unmanned Underwater Vehicles), was identified by 58% of the participants as credible. The results of these survey queries can be seen in more detail in Figures 10–12.

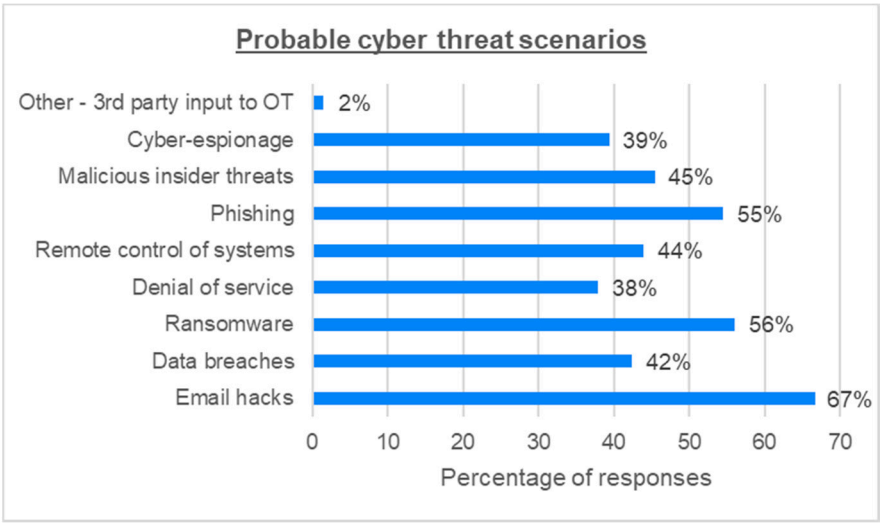


**Figure 10.** Probable cyber threat scenarios.

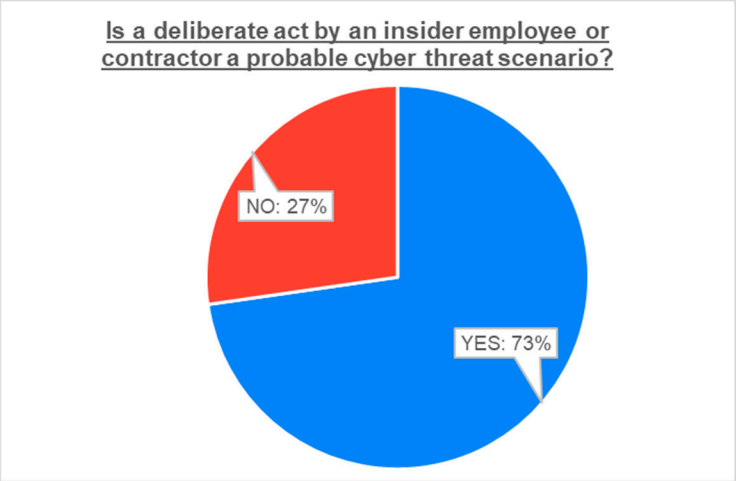


**Figure 11.** Probable cyber threat scenario of insider employee or contractor.

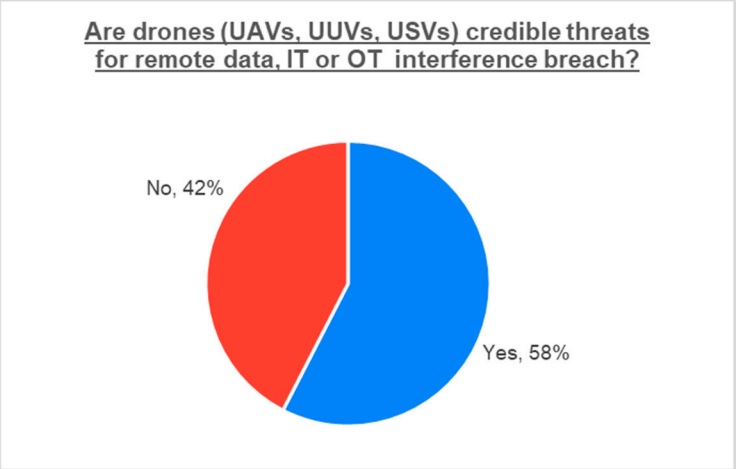


**Figure 12.** Credibility of drones (i.e., UAVs, UUVs, USVs) as threats for IT/OT (operational technology) breach.

For the investigation into the monitoring and integration of cyber security into the operational organization and the built up of resiliency, the permit-to-work system was revealed to be used for cyber-related operations and modifications of IT and OT control systems, as identified by 67% of participants. The performance of cyber security initiatives is being monitored through corporate and operation related key performance indicators (KPIs), as shown by 32% of participants. It should be noted that a majority of 41% of participants outlined that the use or monitoring of KPIs for cyber security compliance, implementation, or performance is not known to them, which indicates a lack of internal communication or nonlinear delegation of performance control duties. It should be highlighted that through the survey (for 65% of the participants), it was shown that resiliency in case of a cyber security breach scenario is integrated into organizations, and that recovery plans are created and implemented as necessary. The above points are shown in Figures 13–15.

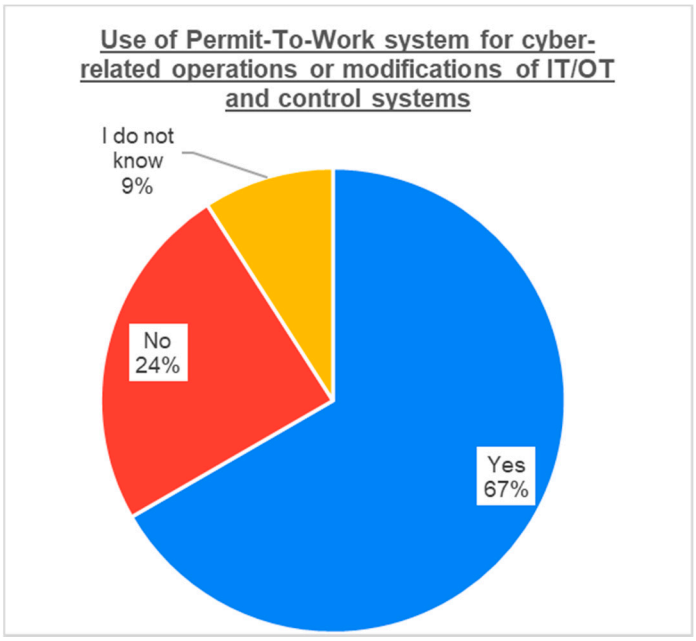


**Figure 13.** Use of permit-to-work system for cyber operations or IT/OT system modifications.

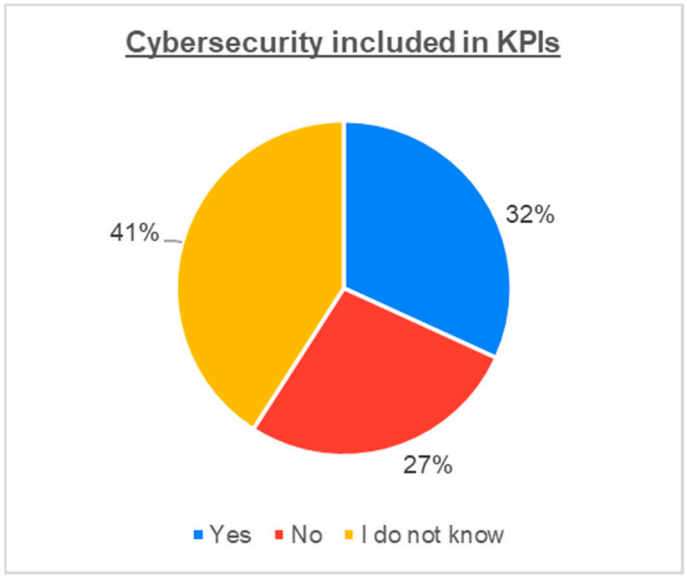


**Figure 14.** Cyber security is included in monitored key performance indicators (KPIs).

From the various standards or directives used by oil and gas companies for cyber security risk assessment and management, 47% of the participants use ISO 27001 standard (Information Security Management), 39% use the International Ship and Port Security (ISPS) code, 39% use API Standard 780 (Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries), and 21% use NIST SP 800-30 (Guide for Conducting Risk Assessments). This indicates the use of diverse standards and tools to mitigate and plan against cyber security threats, covering the industrial, maritime, and IT domain of offshore oil and gas assets. In addition, regarding the organizational or corporate compliance to industry standards or directives for the protection of IT and OT systems, survey participants outlined industry standards ISA 62443, ISA/IEC 62443-4-2, ISA/IC 62443-3-3, and NIST SPP-82 for corporate compliance. The results of the survey are shown in Figures 16 and 17.

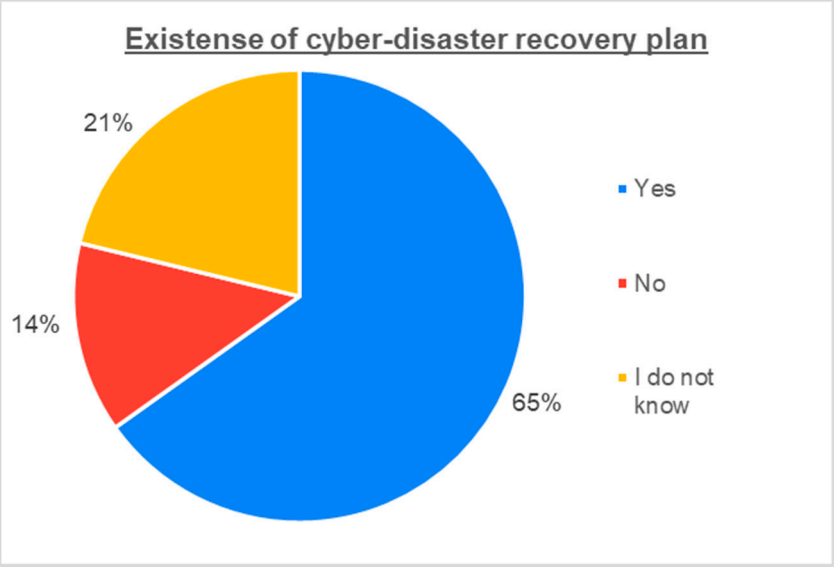


**Figure 15.** Existence of a cyber disaster recovery plan.

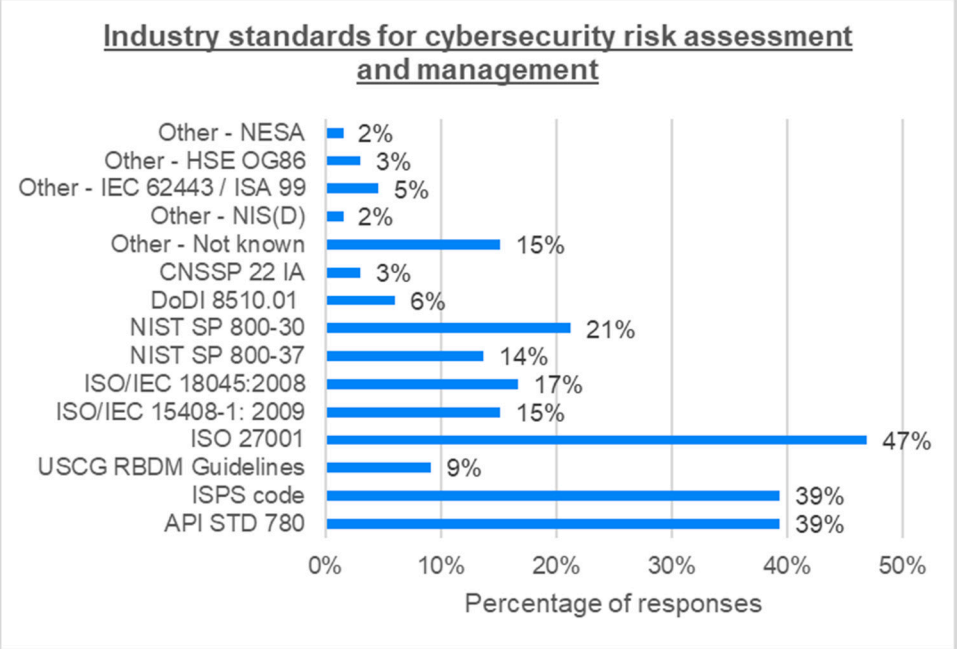


**Figure 16.** Industry standards for cyber security risk assessment and management used by survey participants.

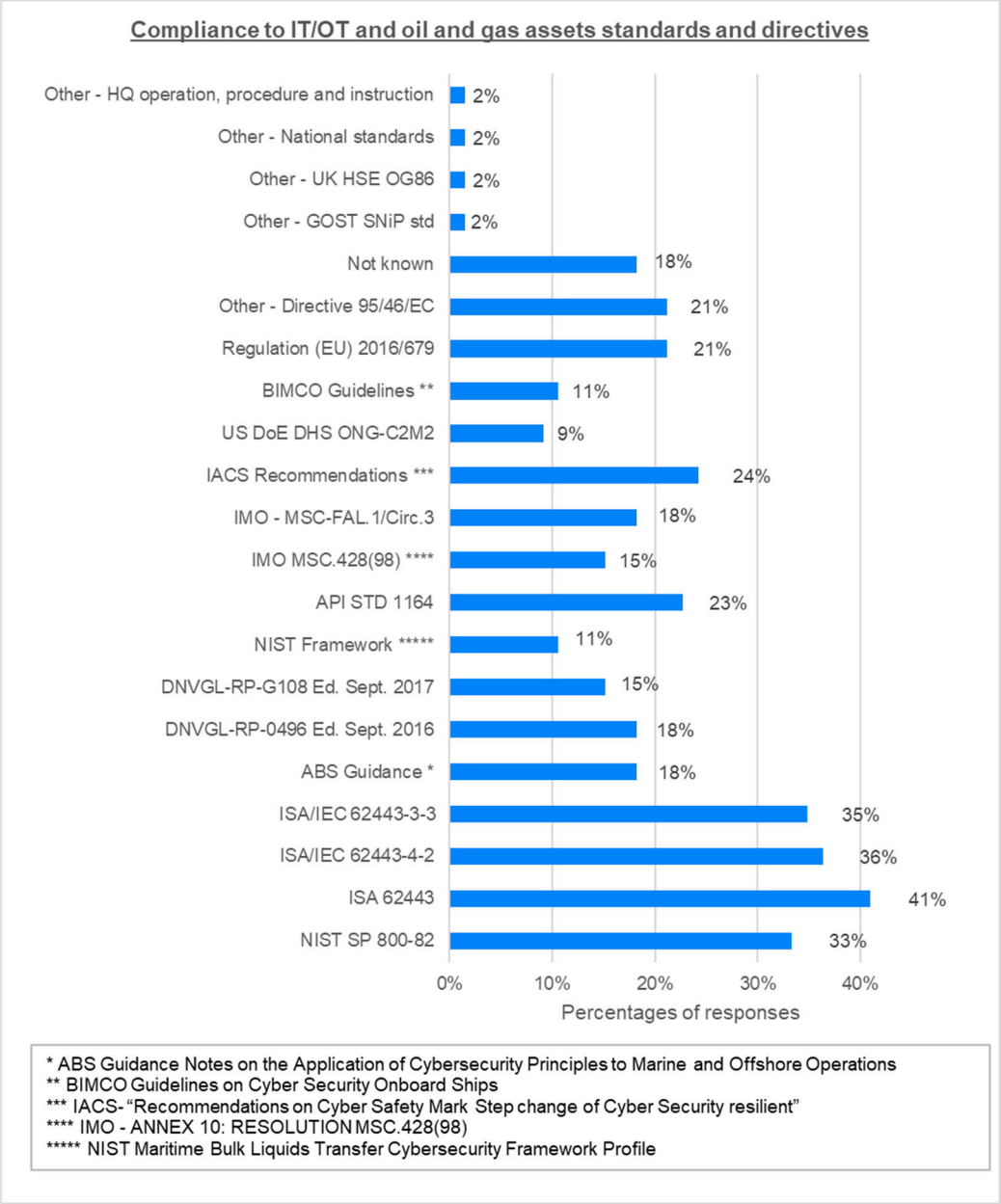


**Figure 17.** Standards and directives for IT/OT for oil and gas assets complied by survey participants.

For the interaction between safety and cyber security, 67% of the participants agreed that there is no conflict between process safety and cyber security requirements, while 91% of participants confirmed that process safety and cyber security are interrelated. These results are presented in Figures 18 and 19.

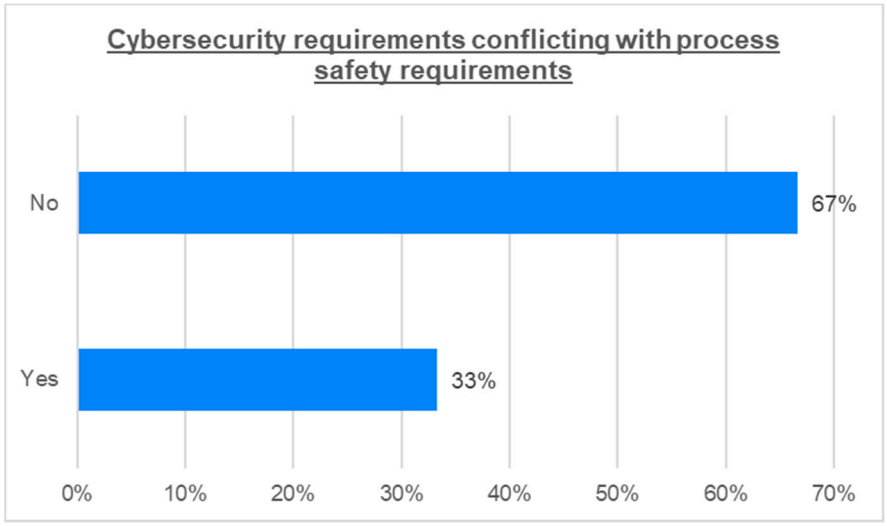


**Figure 18.** Cyber security requirements conflicting with process safety requirements.

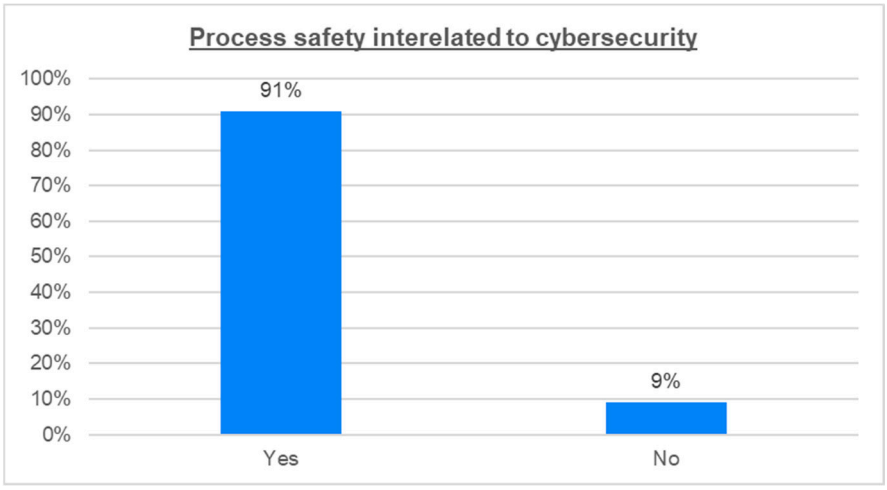


**Figure 19.** Cyber security interrelated to process safety.

Analyzing the proactive or reactive mitigation of cyber security incidents by oil and gas companies and the support they receive to accomplish their goals, 55% of participants confirmed that their company has collaborated with government entities and carried out joint cyber security exercises. In addition, 55% of participants stated that in the case of a cyber security incident, they rely on third-party consultants for the rectification of any damages or malfunctions to their IT and OT systems, and 68% verified that the existing cyber security legislative and directives' framework is sufficient for the mitigation of and preparation against cyber threats. The results of the abovementioned queries are depicted in Figures 20–22.

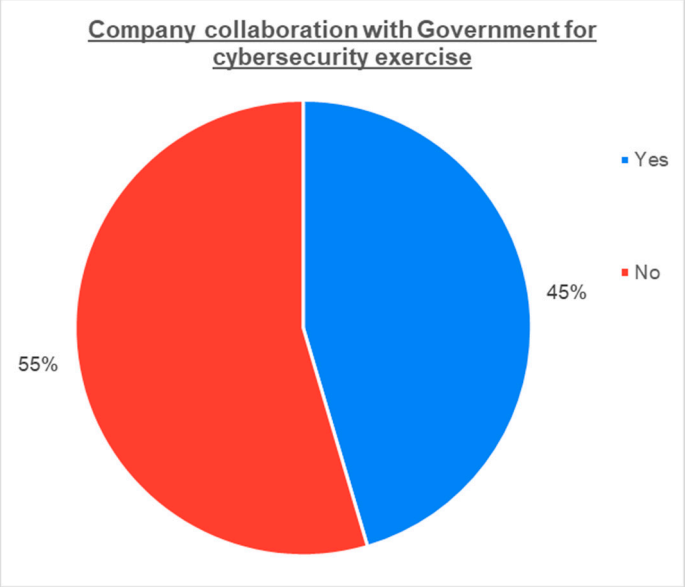


**Figure 20.** Oil and gas companies collaborating with the government for cyber security exercises.

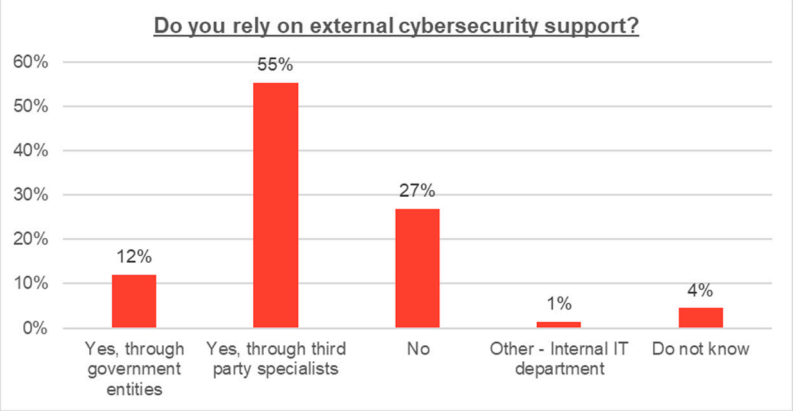


**Figure 21.** External cyber security support provided.

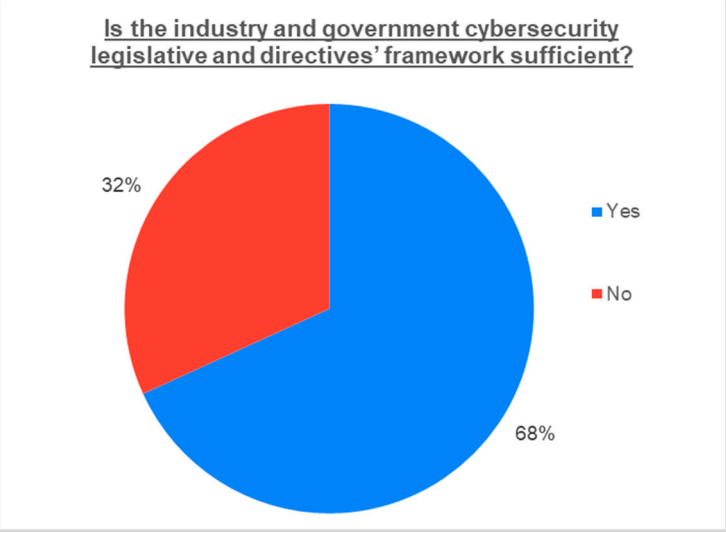


**Figure 22.** Sufficiency of industry and government cyber security legislation and directives.

## 5. Conclusions

From a comparison between Sections 3 and 4, it is evident that there is no direct correlation between the literature review and the industry survey carried out. The identified literature relates to technical aspects involving cyber security while the survey results merely provide a view of participants' perceptions on the subject. Some elements identified in the literature, such as types of threats, vulnerabilities, industry standards, etc., were used in the design of the survey questionnaire. There is, however, no association between the derived survey results and the technical issues raised in the reviewed literature. The identified literature material does not provide quantified analytics that can be compared with the statistical survey results. This proves that the research described in the literature focuses on technical issues rather than on the organizational perception of cyber security threats and their mitigation.

In regard to what has been outlined in Section 4, it is evident that the subject of cyber security has to be viewed and understood through two different spectrums: the human element and the corporate organization. This grading derives from the analysis of results from Figure 8 where the constraints for the implementation of cyber security are presented.

The human element relates to the perceiving and mitigation of threats in the cyber domain at both a technical and operational level as well as a field and managerial level. The survey results indicate that from a wide pool of participants from different locations around the world, the insider threat and the lack of cyber security culture or concept understanding are ranked higher than most other cyber threats. In particular, 73% of the participants acknowledged that the cyber security threat from a malicious insider is probable. This is in agreement with data from other surveys carried out in the subject where similar results, i.e., 78% as found by Williams and Ciepiela [54], are observed. In another survey by Ponemon/Siemens [55], the insider threat is recognized, but 65% of the participants consider the negligent insider threat more probable than the malicious insider one (15%).

The lack of understanding of cyber security principles and its effect in the operations or organization in the case of an incident also pose a very credible threat in the proactive and reactive mitigation of cyber security breach incidents. This is further proven by the acknowledgement of portable USB devices (the most employee-led piece of equipment) and low employee awareness as the greatest cyber security vulnerabilities (67% and 48%, respectively). The lack of awareness was also recognized from other surveys [54], where 43% of the participants identify the lack of end user awareness as a significant threat. The lack of awareness and supportive corporate culture does not apply only to "blue collar" personnel such as field engineers and technicians, but also to the higher management. If cyber security is not fully understood as a concept or as a threat, support for the implementation of cyber security measures, to include technological tools and policies, will not be provided. This is acknowledged by 41% of the survey participants and relates to the financial constraints existing in companies' organization in authorizing the acquiring of new tools and the adoption of new measures.

In the level of corporate organization for the oil and gas sector, the survey results indicate that cyber security is adopted by organizations through the training of personnel (corporate and contractors), the implementation of a variety of proactive or reactive mitigation cyber tools, the proficient understanding of industry standards and certifications in the subject, its incorporation to operational management through the use of the permit-to-work system, and its field monitoring through operational key performance indicators (KPIs). In addition, from the participants' responses, it is revealed that oil and gas companies have a good understanding of the interrelation of safety and cyber security. Survey results reveal that oil and gas companies do have disaster recovery plans, and they either rely on or receive support from external third-party cyber security experts, presumably though contracted services or corporate collaborations. Collaborations between oil and gas companies and governmental organizations is also shown through the participation in joint cyber security exercises.

From the above, one can understand that the subject of cyber security is conflicting in its adaptation and understanding from oil and gas companies and their personnel. On one hand, the implementation of cyber security tools, counter measures, and standards and policies is shown at a corporate and field level. On the other hand though, the lack of understanding of cyber security principles and necessity at a field and corporate level hinders the mitigation of cyber security incidents through the inefficient financial corporate commitment and the negligence and lack of awareness from field personnel on the subject. Unequivocally, the implementation of technical measures is directly affected by the people deciding (i.e., managers) the funding of the necessary tools for cyber security or those specifying and requesting (engineers, technicians, etc.) these tools.

Some suggested organizational and technical measures for the offshore oil and gas domain to tackle cyber security are as follows:

- The adaptation of measures for the mitigation of insider threats: As illustrated from the survey results, insider-led malicious acts rank high in their probability to occur. Their mitigation is considered difficult as they constitute a hybrid type of threats that can include criminal intent, unintentional actions, as well as state sponsored espionage. These measures can be methods and tools used by the military and government sectors that could be replicated to the possible extent in order to tackle these threats in a proactive manner.
- The implementation of countermeasures against hostile unmanned platforms (i.e., UAVs, UUVs, USVs): Unmanned platforms or drones are continuously advancing in performance and technological characteristics and pose a significant threat that can cause electronic interference or even attack against network-connected devices [56]. Countermeasures to be implemented should consider the special operational conditions of offshore oil and gas assets and should not impede the safety of infrastructure, systems, or personnel. These countermeasures can be electronic countermeasures or kinetic-type of weapons that neutralize such airborne, surface, or underwater threats, similar to the ones used by the military or government security agencies.
- The improvement of corporate and industry culture on the perception of cyber security: This is a difficult feat that can be achieved through the study of known attacks in the industry, the sharing of information on such attacks through industry organizations, the increased communication between industry sectors and companies' departments, and the increased and continuous training of individuals on the subject. These are also suggested by government and industry reports from Folga et al. and the Argonne National Laboratory [29].
- The increased monitoring of cyber security performance indicators through the use of corporate KPIs
- The increased collaboration with the government and the military for the training of personnel, simulation of attack scenarios, and general raising of awareness on the subject at a legislative and national security level
- The abolition of USB devices from the available toolkit of the offshore oil and gas domain: This could be achieved by the further integration of IIoT and wireless communication but with their enhanced security features.
- The increased capital and operational expenditure for cyber security measures dictated by industry standards and national legislation: As the offshore oil and gas sector is considered critical for many national economies and supporting numerous others critical infrastructures, it is obvious that funding and resources need to be allocated to increase asset and organizational resiliency.

To conclude, the oil and gas industry has to recognize that cyber security threats are persistent and continuously evolving to be more sophisticated and technologically advanced. In order for oil and gas companies to protect their assets, they need to acknowledge and understand the threat and the necessity for organizational and technical measures to be adopted. Any measures to be considered need to be dynamically evaluated and implemented in order to ensure that oil and gas organizations and their assets are catching

up with the advancement of their cyber adversaries. Resiliency has to be built into the organizational, operational, and technical level of oil and gas companies in order to maximize the possibility of repelling cyber attacks and minimize the technical and corporate consequences of cyber breaches, especially for remote offshore assets. Consideration should also be given to the future evolution of threats through the weaponization of malware and high precision and targeted attacks to critical oil and gas infrastructure and IT/OT systems. Lastly, the parameter of physical security should not be neglected, as its failure or inadequacy can impede insider threat mitigation measures.

## 6. Limitations and Future Work

The authors have attempted to provide an overview of all literature that is relevant to the cyber security aspects of offshore oil and gas assets. It is possible that some literature material may have been missed due to its unavailability at the time of the writing of this article. As cyber security threats evolve and cyber attacks are being more known to the industry, more publications on the subject are being released.

It has to be understood that the technical and operational cyber security vulnerabilities of offshore oil and gas assets are shared to some extent by assets in the midstream and downstream oil and gas sector, the chemical and processing sector, as well as the maritime sector. In order to capture the full spectrum of literature available and validate the commonalities or differences, it would be beneficial to consider an extensive review of such available material in the future.

In order to gain a better understanding of the cyber security technical and operational vulnerabilities of and threats faced by offshore oil and gas assets, the physical security aspects should be further investigated as they directly influence their cyber operations and resiliency.

It has to be acknowledged that the survey questionnaire used for capturing the industry's perception on the subject of cyber security for offshore oil and gas assets involves a risk of receiving biased or incorrect feedback from participants. The quality of the collected data depends on knowledge, experience, and willingness from the participants to share information. This risk was accepted by the authors as it was found that there was no other method to pursue the anonymous collection of information in the subject from a wider pool of participants. The difficulty of determining or certifying the level of knowledge or competence in cyber security for survey participants is also recognized by the authors, considering the structure and design of the used survey questionnaire.

It should be also highlighted that very early at the distribution of the survey questionnaire, a large number of negative responses were received that declined any participation in the dissemination of any information on the aspects of cyber security for offshore oil and gas assets. The subject was considered by many participants in the companies, government, and military as sensitive, as it covers industry confidential and national security information. Many responses were also received from individuals declining to participate in the questionnaire due to their lack of knowledge in the specific subject. Attempts to pursue the distribution of the survey questionnaire by industry organizations such as the IADC (International Association of Drilling Contractors) and IOGP (International Association of Oil and Gas Producers) were unsuccessful. It was thought that if the survey effort had received the endorsement of such organizations, a larger pool of participants could be accessed, which in turn could provide more valuable data. It is recommended that for the collection of more reliable data on the subject, the support or endorsement of industry organizations should be sought.

**Author Contributions:** I.P. conceived the title, idea, and layout of the paper, wrote and edited the draft and final manuscript, and processed survey data; N.N. provided supervision, direction on the layout and structure of the paper, and a review of the survey questionnaire and draft manuscript; P.R., B.B., D.D. and S.K. provided a review of the survey questionnaire and draft manuscript. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** The data presented in this study are available on request from the corresponding author. The data are not publicly available due to confidentiality reasons.

**Acknowledgments:** Iosif Progoulakis would like to acknowledge the support provided by the Fulbright Foundation of Greece for enabling part of this research effort through the awarded Fulbright Scholarship and PhD research visit to the Maritime Security Center (MSC) at the Stevens Institute of Technology (NJ, USA) between September and December 2019.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Eversheds Sutherland Ltd. *Microsoft Report DTUK001917_10/18: Responding to the Evolving Cyber Threat Landscape in the Oil and Gas Sector*; Eversheds Sutherland Ltd.: London, UK, 2018.
2. Coble, S. Attacks Against Oil and Gas Industry on the Rise. Available online: https://www.infosecurity-magazine.com/news/attacks-against-oil-and-gas (accessed on 24 September 2020).
3. Ovcina, J. Naval Dome: 400% Increase in Attempted Hacks Since February 2020. Available online: https://www.offshore-energy.biz/naval-dome-400-increase-in-attempted-hacks-since-february-2020/ (accessed on 10 August 2020).
4. Lu, H.; Guo, L.; Azimi, M.; Huang, K. Oil and Gas 4.0 era: A systematic review and outlook. *Comput. Ind.* **2019**, *111*, 68–90. [CrossRef]
5. Lamb, K. Challenges of Digitalisation in the Offshore Oil and Gas Sector. In *University of Cambridge CMBB Research Bridgehead Report CDBB_REP_001*; Center for Digital Build Britain (CDBB): Cambridge, UK, 2018.
6. Mohammadpoor, M.; Torabi, F. Big Data analytics in oil and gas industry: An emerging trend. *J. Pet.* **2018**. Under Publication. [CrossRef]
7. Nguyen, T.; Gosine, R.G.; Warrian, P. A Systematic Review of Big Data Analytics for Oil and Gas Industry 4.0. *IEEE Access* **2020**, *8*, 61183–61201. [CrossRef]
8. Gharbi, R.B.C.; Mansoori, G.A. An introduction to artificial intelligence applications in petroleum exploration and production. *J. Pet. Sci. Eng.* **2005**, *49*, 93–96. [CrossRef]
9. Bello, O.; Holzmann, J.; Yaqoob, T.; Teodoriu, C. Application of Artificial Intelligence Methods in Drilling System Design and Operations: A Review of the State Of The Art. *J. Artif. Intell. Soft Comput. Res.* **2015**, *5*, 121–139. [CrossRef]
10. LaGrange, E. Developing a Digital Twin: The Roadmap for Oil and Gas Optimization. In Proceedings of the 2019 SPE Offshore Europe Conference and Exhibition, Aberdeen, UK, 3–6 September 2019.
11. Holmås, H.; Sjåtil, O.A.; Santamarta, S.; Lindseth, S.H.; Forbes, P.W.; Romanin, P. *Creating Value with Digital Twins in Oil and Gas*; Boston Consulting Group: Boston, MA, USA, 2019.
12. Thibaud, M.; Chi, H.; Zhou, W.; Piramuthu, S. Internet of things (IoT) in high-risk Environment, Health and Safety (EHS) industries: A comprehensive review. *J. Decis. Support Syst.* **2018**, *108*, 79–95. [CrossRef]
13. Nikitakos, N.; Progoulakis, I. An introduction to the security assessment for offshore oil and gas installations. *NMIOTC MIO J.* **2019**, *18*, 10–18.
14. Lobo, F. *Upstream Oil & Gas Cyber Risk: Insurance Technical Review*; Lloyd's Market Assoc.: London, UK, 2018.
15. Crandal, J. Cybersecurity and Offshore Oil: The Next Big Threat. 4 Oil & Gas. *Nat. Resour. Energy J.* **2019**, *4*, 703–735.
16. Soares, L.; Souza, R. Cyber Risks in the Oil & Gas Industry. In Proceedings of the Rio Oil and Gas Expo and Conference, Rio de Janeiro, Brazil, 15–18 September 2014.
17. Hacquebord, F.; Pernet, C. Drilling Deep: A look at Cyberattacks on the Oil and Gas Industry, Trend Micro Research. 2019. Available online: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/drilling-deep-a-look-at-cyberattacks-on-the-oil-and-gas-industry (accessed on 28 September 2020).
18. Ginter, A. *Secure Operations Technology*; Abterra Technologies Inc.: Calgary, AB, Canada, 2018.
19. Lawrence Livermore National Laboratory (LLNL). Dragonstone Strategy—State of Cybersecurity in the Oil & Natural Gas Sector. In *US Government—Lawrence Livermore National Security LLC Report LLNL-TR-805864*; LLNL: Livermore, CA, USA, 2020.
20. Dragos Inc. Global Oil and Gas Cyber Threat Perspective: Assessing the Threats, Risks, and Activity Groups Affecting the Global Oil and Gas Industry. August 2019. Available online: https://www.dragos.com/wp-content/uploads/Dragos-Oil-and-Gas-Threat-Perspective-2019.pdf (accessed on 1 August 2019).
21. Hadjistassou, C.; Bratskas, R.; Koutras, N.; Kyriakides, A.; Charalambous, E.; Hadjiantonis, A.M. Safeguarding critical infrastructures from cyber attacks: A case study for offshore natural gas assets. *J. Pol. Saf. Reliab. Assoc.* **2015**, *6*, 115–123.
22. Stergiopoulos, G.; Gritzalis, D.A.; Limnaios, E. Cyber-Attacks on the Oil & Gas Sector: A Survey on Incident Assessment and Attack Patterns. *IEEE Access* **2020**, *8*, 128440–128475.

23. Moreno, V.C. Analysis of physical and cyber security-related events in the chemical and process industry. *Process Saf. Environ. Prot.* **2018**, *116*, 621–631. [CrossRef]
24. Rohmeyer, P.; Bayuk, J.L. *Financial Cybersecurity Risk Management*; Springer: Berlin/Heidelberg, Germany, 2019.
25. Fazzini, K. CNBC Tech News. The Saudi Oil Attacks Could Be a Precursor to Widespread Cyberwarfare—With Collateral Damage for Companies in the Region. 2019. Available online: https://www.cnbc.com/2019/09/21/saudi-aramco-attacks-could-predict-cyber-warfare-from-iran.html (accessed on 9 December 2019).
26. Clayton, B.; Segal, A. Council on Foreign Relations Energy Brief: Addressing Cyber Threats to Oil and Gas Suppliers. 2013. Available online: https://www.files.ethz.ch/isn/166056/Energy_Brief_Clayton_Segal.pdf (accessed on 12 September 2020).
27. Deloitte University Press. Protecting the Connected Barrels—Cybersecurity for Upstream Oil and Gas, A Report by Deloitte Center for Energy Solutions, Houston, TX, USA. 2017. Available online: https://www2.deloitte.com/tr/en/pages/energy-and-resources/articles/oil-and-gas-cybersecurity.html (accessed on 27 June 2019).
28. Lewis, T.G. *Critical Infrastructure Protection in Homeland Security*, 3rd ed.; Willey: Hoboken, NJ, USA, 2020.
29. Stephen, F.S.; Talaber, L.; McLamore, M.; Kraucunas, I.; McPherson, T.; Manzanares, T.; Parrott, L. Literature Review and Synthesis for the Natural Gas Infrastructure. In *Argonne National Laboratory Report ANL/GSS-15/5*; Argonne, IL, USA, 2015. Available online: https://www.osti.gov/biblio/1350046 (accessed on 22 January 2021).
30. NTT Security Global Overview: Cybersecurity Expertise in the oil and Gas Sector. In *NTT Security—NTT Group Report*; NTT Group: Tokyo, Japan, 2019.
31. Chevron Says Hit by Stuxnet Virus in 2010. 2012. Available online: https://phys.org/news/2012-11-chevron-stuxnet-virus.html (accessed on 28 September 2020).
32. *ENISA Report ETL2020. Cyber Espionage: ENISA Threat Landscape from January 2019 to April 2020*; ENISA (European Union Agency for Cybersecurity): Athens, Greece, 2020.
33. Katharina Rick and Karthik Lyer, BCG Perspectives: Countering the Threat of Cyberattacks in Oil and Gas. 2016. Available online: https://www.bcg.com/publications/2016/upstream-oil-gas-technology-digital-countering-the-threat-of-cyberattacks-in-oil-and-gas (accessed on 3 December 2019).
34. DNV GL, Cyber Security Vulnerabilities for the Oil and Gas Industry, Lysne Committee Study—Executive Summary. 2015. Available online: https://www.dnvgl.com/oilgas/download/lysne-committee-study.html (accessed on 9 September 2019).
35. Yang, L.; Cao, X.; Li, J. A new cyber security risk evaluation method for oil and gas SCADA based on factor state space. *J. Chaos Solitons Fractals* **2015**, *89*, 203–209. [CrossRef]
36. Vieira, A.C.; Houmb, S.H.; Insua, D.R. *A Graphical Adversarial Risk Analysis Model for Oil and Gas Drilling Cybersecurity*; GraMSec: Grenoble, France, 2014; pp. 78–93.
37. Siva Prasad, M.V.V.; Avadhani, P.S. Attack Tree Design and Analysis of Offshore Oil and Gas Process Complex SCADA System. *Int. J. Comput. Appl.* **2019**, *181*, 12–18.
38. Refsdal, A.; Solhaug, B.; Stølen, K. Security risk analysis of system changes exemplified within the oil and gas domain. *Int. J. Softw. Tools Technol. Transf.* **2015**, *17*, 251–266. [CrossRef]
39. Marcin, Ś.; Emilian, P. Procedure based functional safety and information security management of industrial automation and control systems on example of the oil port installations. *J. Pol. Saf. Reliab. Assoc.* **2017**, *8*, 129–138.
40. Kosmowski, K.T.; Gołębiewski, D. Functional safety and cyber security analysis for life cycle management of industrial control systems in hazardous plants and oil port critical infrastructure including insurance. *J. Pol. Saf. Reliab. Assoc.* **2019**, *10*, 99–126.
41. McEvoy, T.R.; Wolthusen, S. An Attack Analysis of Managed Pressure Drilling Systems on Oil Drilling Platforms. In Proceedings of the International Conference on Critical Information Infrastructures Security CRITIS 2014, Berlin, Germany, 2–3 September 2014; pp. 109–121.
42. Fataliyev, T.K.; Mehdiyev, S.A. Analysis and New Approaches to the Solution of Problems of Operation of Oil and Gas Complex as Cyber-Physical System. *Inf. Technol. Comput. Sci.* **2018**, *11*, 67–76. [CrossRef]
43. Aalsalem, M.Y.; Khan, W.Z.; Gharibi, W.; Khan, M.K.; Arshad, Q. Wireless Sensor Networks in oil and gas industry: Recent advances, taxonomy, requirements, and open challenges. *J. Netw. Comput. Appl.* **2018**, *113*, 87–97. [CrossRef]
44. Radmand, P.; Talevski1, A.; Petersen, S.; Carlsen, S. Taxonomy of Wireless Sensor Network Cyber Security Attacks in the Oil and Gas Industries. In Proceedings of the 2010 24th IEEE International Conference on Advanced Information Networking and Applications, Perth, WA, Australia, 20–23 April 2010; pp. 949–957.
45. Sveen, F.O.; Qian, Y.; Hillen, S.; Radianti, J.; Gonzalez, J.J.; Dynamic, A. Approach to Vulnerability and Risk Analysis of the Transition to eOperations. In Proceedings of the 24th International Conference of the System Dynamics Society, Nijmegen, The Netherlands, 23–27 July 2006.
46. Rydzak, F.; Breistrand, L.; Sveen, F.O.; Qian, Y.; Gonzalez, J.J. Exploring resilience towards risks in eOperations in the oil and gas industry. In Proceedings of the 25th international conference on Computer Safety, Reliability, and Security SAFECOMP'06, Gdansk, Poland, 27–29 September 2006; pp. 57–70.
47. Spandonidis, C.C.; Giordamlis, C. Data-centric Operations in Oil & Gas Industry by the Use of 5G Mobile Networks and Industrial Internet of Things (IIoT). In Proceedings of the Thirteenth International Conference on Digital Telecommunications ICDT, Athens, Greece, 22–26 April 2018.
48. Erkoyuncu, J.A.; Ononiwu, S.; Roy, R. Mitigating the Risk of Software Obsolescence in the Oil and Gas Sector. In Proceedings of the 3rd International Conference on Through-life Engineering Services, Procedia CIRP 22, Cranfield, UK, 2–4 July 2014; pp. 81–86.

49. *ENISA Report, Report on Cyber Security Information Sharing in the Energy Sector*; ENISA (European Union Agency for Cybersecurity): Athens, Greece, 2016.
50. Holcomb, J. Definitive Guide to Cybersecurity for the Oil & Gas Industry. In *LEIDOS Ebook Report*; LEIDOS Holdings Inc.: Reston, VA, USA, 2016. Available online: https://www.ciosummits.com/Online_Assets_Leidos_Definitive_Guide_to_Cyber_for_Oil_and_Gas_eBook.pdf (accessed on 17 January 2021).
51. Oil and Natural Gas Subsector Coordinating Council (ONG SCC); Natural Gas Council (NGC). Defense-in-Depth: Cybersecurity in the Natural Gas and Oil Industry. In *ONG SCC and NGC Report*; Washington, DC, USA, 2018. Available online: http://ongsubsector.com/ (accessed on 22 January 2021).
52. Sam Chambers, Number of Shipping Cyber Attacks Leaps 400% Since February. Available online: https://splash247.com/number-of-shipping-cyber-attacks-leaps-400-since-february/ (accessed on 6 July 2020).
53. David Paul, Weathering the Storm: The Oil and Gas Sector and COVID-19. Available online: https://digit.fyi/weathering-the-storm-the-oil-and-gas-sector-and-covid-19/ (accessed on 15 June 2020).
54. Jeff Williams and Piotr Ciepiela, Six Cybersecurity Issues for Oil and Gas Companies. 2019. Available online: https://www.ey.com/en_gl/oil-gas/six-cybersecurity-issues-for-oil-and-gas-companies (accessed on 12 November 2019).
55. Ponemon Institure LLC/SIEMENS, The State of Cybersecurity in the Oil & Gas Industry: United States. 2017. Available online: https://assets.siemens-energy.com/siemens/assets/api/uuid:4ec3d46c-234e-4f48-9bc7-aef5889dcaba/ponemoncyberreadinessinoilgasfinal.pdf (accessed on 23 August 2020).
56. Katharina, L.B. How to Analyze the Cyber Threat from Drones. In *RAND Report RR2972*; RAND Corp.: Santa Monica, CA, USA, 2020.