International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 8 Issue 5, Sep-Oct 2024 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Cybersecurity in Oil and Gas Industry

Matthew N. O. Sadiku[1], Paul A. Adekunte[2], Janet O. Sadiku[3]

[1]Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, TX, USA
[2]International Institute of Professional Security, Lagos, Nigeria
[3]Juliana King University, Houston, TX, USA

ABSTRACT

Oil and gas (O&G) companies deal with vast amounts of sensitive information, and protecting it is vital to prevent financial loss, reputational damage, and regulatory non-compliance. Playing a vital role in the global economy, the oil and gas industry is a prime cyber threat target. A cyberattack on O&G critical infrastructure could cause physical, environmental, and economic harm and broad disruptions to oil and gas supplies and markets. Cybersecurity is paramount for the oil and gas industry as it plays a critical role in securing the sensitive data and operational technology that enables the industry to extract, produce, and transport oil and gas. The paper focuses on systematically exploring cybersecurity and safety challenges of the O&G sector.

KEYWORDS: *oil & gas industry, petrochemical industry, security, cybersecurity*

How to cite this paper: Matthew N. O. Sadiku | Paul A. Adekunte | Janet O. Sadiku "Cybersecurity in Oil and Gas Industry" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-8 | Issue-5, October 2024, pp.830-838, URL: www.ijtsrd.com/papers/ijtsrd69459.pdf

IJTSRD69459

Copyright © 2024 by author (s) and International Journal of Trend in Scientific Research and Development Journal. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0) (http://creativecommons.org/licenses/by/4.0)

IJTSRD International Journal of Trend in Scientific Research and Development ISSN: 2456-6470

INTRODUCTION

The oil and gas industry is a prime target for cyber-attacks due to the high value of the data and systems they control. Cyber attacks on the oil and gas industry are growing because the sector is becoming increasingly dependent on technology and automation. The industry's production, transportation, and refining processes rely heavily on control systems connected to the Internet, making them vulnerable to cyber threats [1]. Oil and gas companies, being critical infrastructure, can become prime targets for state-sponsored or politically motivated cyber groups aiming to disrupt operations, steal sensitive data, or cause economic damage. Gas producers may face a range of security risks, from production shutdowns to inaccessibility. This could result in long-term shortages [2].

Cybersecurity is a critical aspect of the oil and gas industry because it protects the sensitive data and operational technology that the industry relies on. Oil and gas operations involve critical infrastructure such as refineries, pipelines, and drilling rigs. These operations are vulnerable to cyberattacks. The consequences of successful cyberattacks can be severe, leading to physical damage, production disruptions, environmental disasters, and significant financial losses.

OVERVIEW ON CYBERSECURITY

Cybersecurity refers to a set of technologies and practices designed to protect networks and information from damage or unauthorized access. It is vital because governments, companies, and military organizations collect, process, and store a lot of data. As shown in Figure 1, cybersecurity involves multiple issues related to people, process, and technology [3]. Figure 2 shows different components of cybersecurity [4].

A typical cyber attack is an attempt by adversaries or cybercriminals to gain access to and modify their target's computer system or network. Cybercriminals or ethical hackers are modern-day digital warriors, possessing extraordinary skills and knowledge to breach even the most impregnable systems. A typical cybercriminal is shown on Figure 3 [5]. Cyber attacks are becoming more frequent, sophisticated, dangerous, and destructive. They are threatening the operation of businesses, banks, companies, and government networks. They vary from illegal crime of individual citizen (hacking) to actions of groups (terrorists) [6].

The cybersecurity is a dynamic, interdisciplinary field involving information systems, computer science, and criminology. The security objectives have been availability, authentication, confidentiality, nonrepudiation, and integrity. A security incident is an act that threatens the confidentiality, integrity, or availability of information assets and systems [7].

- *Availability*: This refers to availability of information and ensuring that authorized parties can access the information when needed. Attacks targeting availability of service generally leads to denial of service.
- *Authenticity*: This ensures that the identity of an individual user or system is the identity claimed. This usually involves using username and password to validate the identity of the user. It may also take the form of what you have such as a driver's license, an RSA token, or a smart card.
- *Integrity*: Data integrity means information is authentic and complete. This assures that data, devices, and processes are free from tampering. Data should be free from injection, deletion, or corruption. When integrity is targeted, nonrepudiation is also affected.
- *Confidentiality*: Confidentiality ensures that measures are taken to prevent sensitive information from reaching the wrong persons. Data secrecy is important especially for privacy-sensitive data such as user personal information and meter readings.
- *Nonrepudiation*: This is an assurance of the responsibility to an action. The source should not be able to deny having sent a message, while the destination should not deny having received it. This security objective is essential for accountability and liability.

Everybody is at risk for a cyber attack. Cyber attacks vary from illegal crime of individual citizen (hacking) to actions of groups (terrorists). The following are typical examples of cyber attacks or threats [8]:

- *Malware*: This is a malicious software or code that includes traditional computer viruses, computer worms, and Trojan horse programs. Malware can infiltrate your network through the Internet, downloads, attachments, email, social media, and other platforms. Spyware is a type of malware that collects information without the victim's knowledge.
- *Phishing*: Criminals trick victims into handing over their personal information such as online passwords, social security number, and credit card numbers.
- *Denial-of-Service Attacks*: These are designed to make a network resource unavailable to its intended users. These can prevent the user from accessing email, websites, online accounts or other services.
- *Social Engineering Attacks*: A cyber criminal attempts to trick users to disclose sensitive information. A social engineer aims to convince a user through impersonation to disclose secrets such as passwords, card numbers, or social security number.
- *Man-In-the-Middle Attack*: This is a cyber attack where a malicious attacker secretly inserts him/herself into a conversation between two parties who believe they are directly communicating with each other. A common example of man-in-the-middle attacks is eavesdropping. The goal of such an attack is to steal personal information.

These and other cyber attacks or threats are shown in Figure 4 [9].

The social and financial importance of cybersecurity is increasingly being recognized by businesses, organizations, and governments. Cybersecurity involves reducing the risk of cyber attacks. Cyber risks should be managed proactively by the management. Cybersecurity technologies such as firewalls are widely available [10]. Cybersecurity is the joint responsibility of all relevant stakeholders including government, business, infrastructure owners, and users. Cybersecurity experts have shown that passwords are highly vulnerable to cyber threats, compromising personal data, credit card records, and even social security numbers. Governments and international organizations play a key role in cybersecurity issues. Securing the cyberspace is of high priority to the US Department of Homeland Security (DHS). Vendors that offer mobile security solutions include Zimperium, MobileIron Skycure, Lookout, and Wandera.

CYBERSECURITY IN OIL AND GAS INDUSTRY

The oil and gas industry relies on complex technological systems to facilitate worldwide operations, making it highly vulnerable to cyber threats. Imagine the vast scope of the oil and gas industry: millions of miles of pipes, tankers traveling between ports, hundreds of refineries, rigs, production sites, and headquarters. The oil and gas supply chain is a globally interconnected environment, moving millions of barrels of crude oil and billions of cubic feet of natural gas on a daily basis. The complexity of the O&G systems is typically demonstrated in Figure 5 [11]. The oil and gas infrastructure is a tightly-knit network of extraction, production, refining, and distribution. The oil and gas industry is a prime target for cyber-attacks because of the value of the data and systems it controls. Any disruption can have major socioeconomic consequences due to cyber threats ranging from a data leak to tampering with control systems. Cyber breaches can compromise safety systems, leading to accidents, injuries, and potential environmental disasters.

Five common cyber attacks on the oil and gas industry include [1]:

1. *Phishing*: This type of attack involves sending emails or messages that appear to come from a legitimate source.
2. *Ransomware*: This type of attack involves malware that encrypts the victim's files and demands payment or ransom in exchange for the decryption key.
3. *Advanced Persistent Threats (APTs):* These are long-term, targeted attacks often conducted by nation-states or other highly-skilled actors.
4. *Distributed Denial of Service (DDoS) Attacks:* These attacks involve overwhelming a website or network with traffic to make it unavailable to legitimate users.
5. *Industrial Control Systems (ICS) Attacks*: These attacks target the control systems that operate industrial processes, such as those used in oil and gas production.

The O&G industry faces many challenges in the service sectors of exploration and production. It is segmented into (upstream); processing, storage and transport (midstream); refining and processing (downstream).

- *Upstream Segment*: Upstream stages (exploration, development, and production and abandonment) have a distinct cyber vulnerability, and severity profile. Among the upstream operations, development drilling and production have the highest cyber risk profiles. The oil and gas production operation ranks highest on cyber vulnerability in upstream operations, mainly because of its legacy asset base, which was not built for cybersecurity but has been retrofitted and patched in bits and pieces over the years. A holistic risk management program could not only mitigate cyber risks for the most vulnerable operations but also enable all three of an upstream company's operational imperatives: safety of people, reliability of operations, and creation of new value. Apart from the upstream industry's "critical infrastructure" status, a complex ecosystem of computation, networking, and physical operational processes spread around the world makes the industry highly vulnerable to cyber-attacks. Figure 6 shows cyber vulnerability by upstream operations [12].
- *Downstream Segment:* Cyber attacks can specifically impact the company's downstream business, which includes refining, chemical production, and distribution of petroleum products. Implementation of new technical and operational solutions in upstream and downstream processes was identified as the way forward towards digital oil fields since the early 2000s. For example, in downstream refineries, OT updates typically work around outage schedules so changes take much longer to implement in the oil & gas industry since facilities often operate 24/7.

ROLES OF CYBERSECURITY IN OIL AND GAS

As critical national infrastructure, oil and gas companies are key targets for cybercriminals. Cyberattacks are becoming more and more frequent and more sophisticated. These attacks is not only planned to disrupt operations, but also to cause physical damage threatening human lives. Cybercriminals continue to look for new and innovative ways to infiltrate organizations. Their most common motive is to make money. Other motives of hackers range from cyberterrorism to industry espionage to disrupting operations to stealing field data.

Cyberattacks can compromise the availability, integrity, and confidentiality of oil and gas companies. They can endanger lives. Information systems (IT) and operational technology (OT) are also at risk. Their protection is crucial since it ensures the safety of people, systems, and data. The roles of oil and gas cybersecurity can be summarized as follows [13]:

- *Insider Threats*: Cyber threats are not strictly external; internal threats pose a significant risk as well. Unauthorized physical access to critical infrastructure can result in tampering or destruction of systems. Other so-called insider threats pose a significant challenge, as disgruntled employees, contractors, or others who have been granted prior authorized access can intentionally or unintentionally compromise critical systems and data. Cybercriminals regularly target workers with deceptive emails (i.e., phishing), compromising their credentials or tricking them into installing malware.

- *Supply Chain Risks:* Oil and gas professionals rank inadequate oversight of the vulnerabilities of supply chain partners connected to their organization's environment as the greatest challenge in enhancing OT cybersecurity. A supply chain attack on an oil and gas company is a cyber attack that targets the company's suppliers, vendors, or other partners to gain access to the company's systems and sensitive information. This can be done by compromising the security of a supplier or vendor and then using that access to move deeper into the company's network. The interconnected nature of the oil and gas industry introduces weaknesses through third-party vendors and suppliers. Those armed with privileged access can exploit vulnerabilities, compromise systems, or inadvertently expose critical information.
- *Layered Defense:* There is the need for active defenses and layers of protection for their most important assets. Companies can implement layers of protection for their most important assets. A layered defense, also called "defense in depth," is a proven concept based on various types of overlapping cybersecurity controls. The idea is that if one control fails or gets bypassed by the attacker, another layer offers protection. Companies can also implement active defenses like cyber intelligence, vulnerability awareness, and asset monitoring. Understanding the primary cybersecurity threats comes as the first step in building a robust defense.
- *Data Security:* Security-related data naturally claims for an extremely high degree of sensitivity. This has resulted in major practical limitations in sharing data related to historical events and incidents related to cybersecurity in most cases. Oil and gas companies store large amounts of sensitive data, including intellectual property, financial records, exploration data, and customer information. Protecting this data is essential to prevent financial loss, reputational damage, and regulatory non-compliance. Sensitive data related to operations, production, and financial information needs to be protected from breaches, as this could expose valuable trade secrets and impact market competitiveness.
- *Encryption:* End-to-end encryption on all devices should be required and include embedded security. In some cases, certificate pinning must be required to avoid spoofed devices and this includes protection from side channel attacks that can compromise encryption keys.

BENEFITS

Companies in the oil and gas industry are attractive targets to cybercriminals because energy infrastructure is critical to modern economies. The disruption of an oil or gas pipeline has dire ripple effects on fuel prices, supply chains, and large-scale manufacturing. Building cyber resilience for your organization refers to its ability to survive and protect itself of a cyber-attack. By embracing these best practices, oil and gas companies will be well-positioned to fortify their cyber defenses, securing their critical infrastructure from would-be attackers. Energy companies must take strict measures to counter security threats. Benefits of these measures include the following [14]:

- *Automation*: Automate routine security tasks and orchestrate responses to reduce the burden on security teams, enabling them to focus on critical incidents and respond more efficiently. Implementing a security information and event management system to consolidate and correlate security events across your organization helps to significantly streamline alert management. Implementing automation and machine learning will filter alerts based on their severity and relevance. Your team is then able to analyze them in real-time, reduce false positives, and prioritize critical alerts for immediate attention.
- *Safety:* Increasing focus on safety integrity and the need for new preventative measures to safeguard against new safety risks have resulted in some new interests lately on both fault and failure diagnosis processes related to safety critical systems and equipment of offshore assets.
- *Security:* In the industrial world, productivity drives business. Today, there are security devices with industrialized hardware and advanced configuration options can provide a defense-in-depth option for critical applications. These devices have sophisticated security capabilities including firewalls with integrated router and VPN. Leading the charge in the oil and gas security and service market are major players such as Cisco Systems Inc., Honeywell International Inc., and Siemens. To avoid disruption of services and serious consequences, it is important to take a proactive stance on security, which starts with mitigating the risk of insignificant issues, long before they become major incidents. Companies should try to

implement a platform that integrates physical security (CCTV, access control) with network security (firewalls, intrusion detection) and edge device management. This allows for continuous monitoring and detection of anomalous activity across all layers.

- *Monitoring:* For oil and gas organizations, modern video surveillance, which can be installed at any location, is required to better protect employees, assets, and the natural environment. Ideally, video surveillance is integrated with systems, such as access control, video analytics, and intrusion detection to detect threats faster. It is also important to deploy high-definition IP cameras and thermal imaging cameras to detect what can go unnoticed by regular surveillance.

CHALLENGES

The oil and gas industry faces significant cybersecurity challenges due to its reliance on increasingly interconnected IT and OT systems. Addressing these challenges and enhancing oil and gas cybersecurity is crucial to safeguard critical infrastructure, protect intellectual property, ensure safety, ensure business continuity, prevent cyber threats, and manage supply chain risk. Although emerging technologies will have a major impact on cybersecurity, they can be used for good and also for bad. Other challenges include the following [13]:

- *Worker Awareness:* Knowledge lays the foundation for secure processes and successful access management, and it also raises the awareness of all personnel. Raising oil and gas cybersecurity awareness among your staff helps foster a culture of safety, ensuring everyone understands their roles and responsibilities. With regular training programs, everyone should be periodically tested to eliminate complacency and inertia.

- *Cybersecurity Culture:* A new cybersecurity culture is an important industrial need that should be developed based on central attributes from different domains. The need for such a well-cultivated cybersecurity culture is immediate in all high-risk industrial sectors, such as the offshore O&G industry. Threats are constantly evolving and administering a culture of continuous improvement is one key step toward adopting a cybersecurity strategy that really works. Human factor is often considered as a weak point in the cybersecurity domain and hence the traditional approach of establishing cybersecurity culture often has a focus on raising human and organizational alertness.

- *Reducing Alert Fatigue*: Security alert fatigue is a common challenge for organizations juggling a large volume of warnings. In the oil and gas industry, reducing alert fatigue is an important factor in ensuring legitimate threats are promptly identified and addressed. Reduce alert fatigue by educating all workers, including upper management, about best practices for oil and gas security, thereby raising awareness about the potential consequences of being inattentive to the wide variety of cyber threats your organization regularly faces.

- *Standard:* Oil and gas companies need to constantly raise their standards. They must ask themselves whether they are learning and whether they are doing the right things. This internal scrutiny can be a source of confidence for companies. In 2018, the National Institute of Standards and Technology (NIST) proposes a cybersecurity framework (CSF) constituting of five steps: identify, protect, detect, respond and recover from a security incident. The CSF approach provides an effective framework for the simple integration of various standards, guidelines, and practices within the domains of industrial asset management and cyber risk management. Protecting control systems will be an ongoing responsibility that everyone must share by following standards and implementing a defense-in-depth approach to cybersecurity.

- *Regulation:* Regulatory requirements are the foremost driver of investment in cybersecurity within the oil and gas sector and the wider energy industry.

- *Collaboration*: It is paramount that oil and gas companies stay one step ahead of potential risks. Critical to staying ahead is fostering a culture of industry-wide collaboration. Frequently exchanging threat intelligence with international bodies and developing robust cybersecurity defenses can effectively mitigate cyber risks. To create a secure network, control engineers and plant managers must work together with the IT department and the technology they use.

CONCLUSION

The oil and gas companies play a crucial role in a functional, modern society. The companies face cyber threats daily, from hydrocarbon installation terrorism to industrial espionage. They are also vulnerable to theft and sabotage. Cybersecurity is paramount for the oil and gas industry as it plays a critical role in securing the sensitive data. Ensuring the integrity, confidentiality, and availability of the sensitive data and systems is of utmost importance. Cybersecurity of industrial control systems is multidisciplinary and involves multiple stakeholders, including operator companies, vendors, service providers, authorities, adversaries, and sometimes the public. Holistic cybersecurity ensures people, systems, critical infrastructure, and data are kept safe from cyberattacks.

Oil and gas companies that maintain cybersecurity as a central tenet of their digital strategy stand to gain the most. Emphasizing cybersecurity today means a more secure and resilient oil and gas infrastructure tomorrow. The defense against cyberattacks in oil and gas will have to be taken more seriously in the future. More information on cybersecurity in O&G industry is available from the books in [15-18] and the following related journals:

- *Energy and AI*
- *The AI Journal*

REFERENCES

[1] "Cyber threats for the oil and gas industry," https://meriplex.com/cyber-threats-for-the-oil-and-gas-industry/

[2] G. Lewis, "Mideast oil & gas facilities could face cyber-related energy disruptions," November 2023, https://www.darkreading.com/ics-ot-security/mideast-oil-gas-facilities-could-face-cyber-related-energy-disruptions

[3] P. Singh, "A layered approach to cybersecurity: People, processes, and technology- explored & explained," July 2021, https://www.linkedin.com/pulse/layered-approach-cybersecurity-people-processes-singh-casp-cisc-ces

[4] M. Loi et al., "Cybersecurity in health – disentangling value tensions," *Journal of Information, Communication and Ethics in Society,* June 2019, https://www.emerald.com/insight/content/doi/10.1108/JICES-12-2018-0095/full/html

[5] M. Adams, "Unlocking the benefits of ethical hacking: The importance of ethical hackers in cybersecurity," April 2023, https://www.businesstechweekly.com/cybersecurity/network-security/ethical-hacking/

[6] M. N. O. Sadiku, S. Alam, S. M. Musa, and C. M. Akujuobi, "A primer on cybersecurity," *International Journal of Advances in Scientific Research and Engineering*, vol. 3, no. 8, Sept. 2017, pp. 71-74.

[7] M. N. O. Sadiku, M. Tembely, and S. M. Musa, "Smart grid cybersecurity," *Journal of Multidisciplinary Engineering Science and Technology*, vol. 3, no. 9, September 2016, pp.5574-5576.

[8] "FCC Small Biz Cyber Planning Guide," https://transition.fcc.gov/cyber/cyberplanner.pdf

[9] "The 8 most common cybersecurity attacks to be aware of," https://edafio.com/blog/the-8-most-common-cybersecurity-attacks-to-be-aware-of/

[10] Y. Zhang, "Cybersecurity and reliability of electric power grids in an interdependent cyber-physical environment," *Doctoral Dissertation,* University of Toledo, 2015.

[11] "Strengthening cybersecurity in the oil and gas industry," September 2024, https://www.weforum.org/impact/cyber-resilience-oil-and-gas/

[12] "Protecting the connected barrels: Cybersecurity for upstream oil and gas," https://www2.deloitte.com/content/dam/insights/us/articles/3960-connected-barrels/DUP_Protecting-the-connected-barrels.pdf

[13] "Why is cybersecurity important for oil and gas?" July 2024, https://www.otorio.com/blog/why-is-cybersecurity-important-for-oil-and-gas/

[14] P. Murchland, "Cybersecurity challenges in the energy industry – Are you ready?" July 2024, Unknown Source.

[15] M. N. O. Sadiku, *Cybersecurity and Its Applications.* Moldova, Europe: Lambert Academic Publishing, 2023.

[16] D. J. Lester, *Securing Oil and Natural Gas Infrastructures in the New Economy*. National Petroleum Council, 2001.

[17] C. Sundararaman, *Development of Cybersecurity Mandate For Oil And Gas Industry.* Self Publisher, 2023.

[18] A. Lamba, *Protecting 'Cybersecurity & Resiliency' of Nation's Critical Infrastructure - Energy, Oil & Gas*. SSRN, 2019.

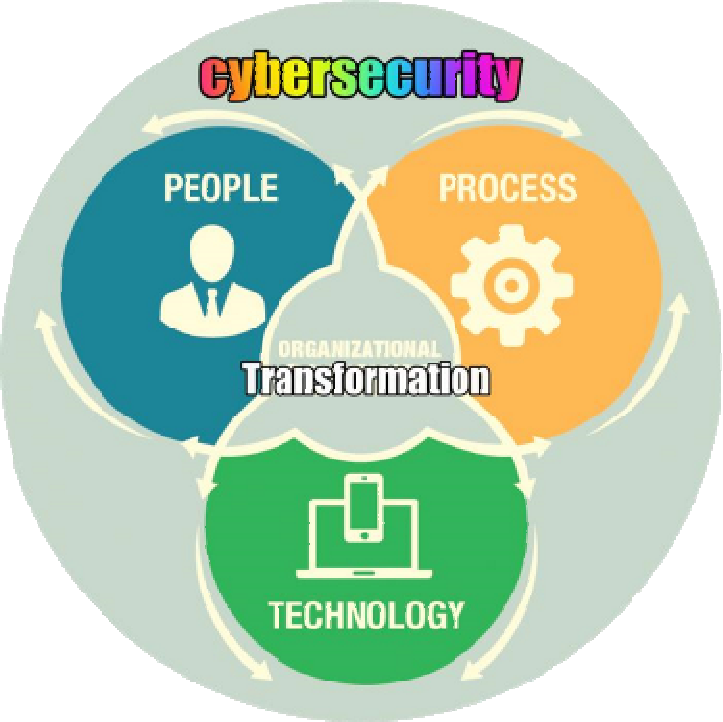
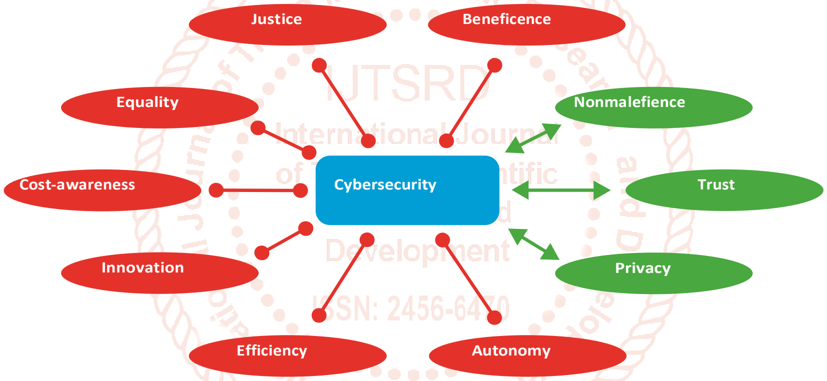


Figure 1 Cybersecurity involves multiple issues related to people, process, and technology [3].



IJTSRD International Journal of Trend in Scientific Research and Development ISSN: 2456-6470

Figure 2 Different components of cybersecurity [4].(Green: supportive; red: in tension)

Figure 3 A typical cybercriminal [5].

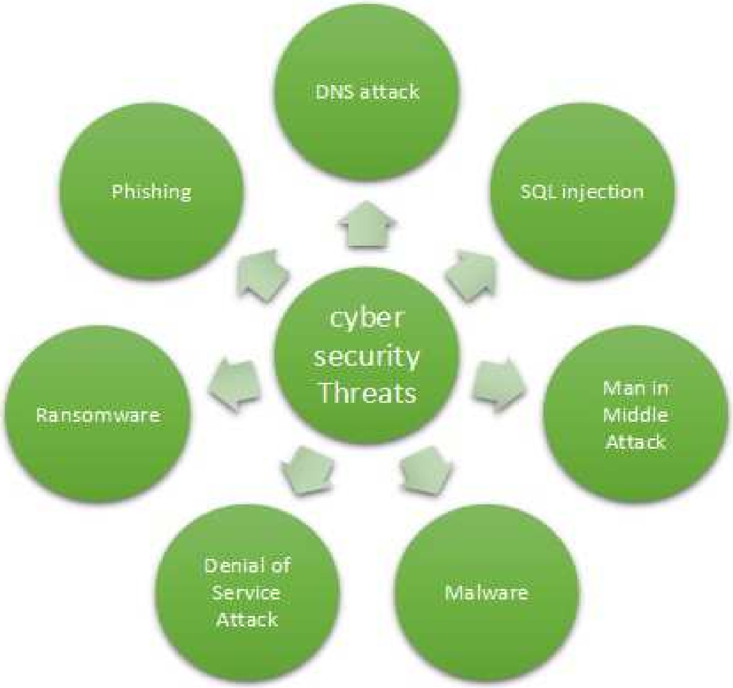


Figure 4 Common types of cybersecurity threats [9].

Figure 5 The complexity of the O&G systems [11].

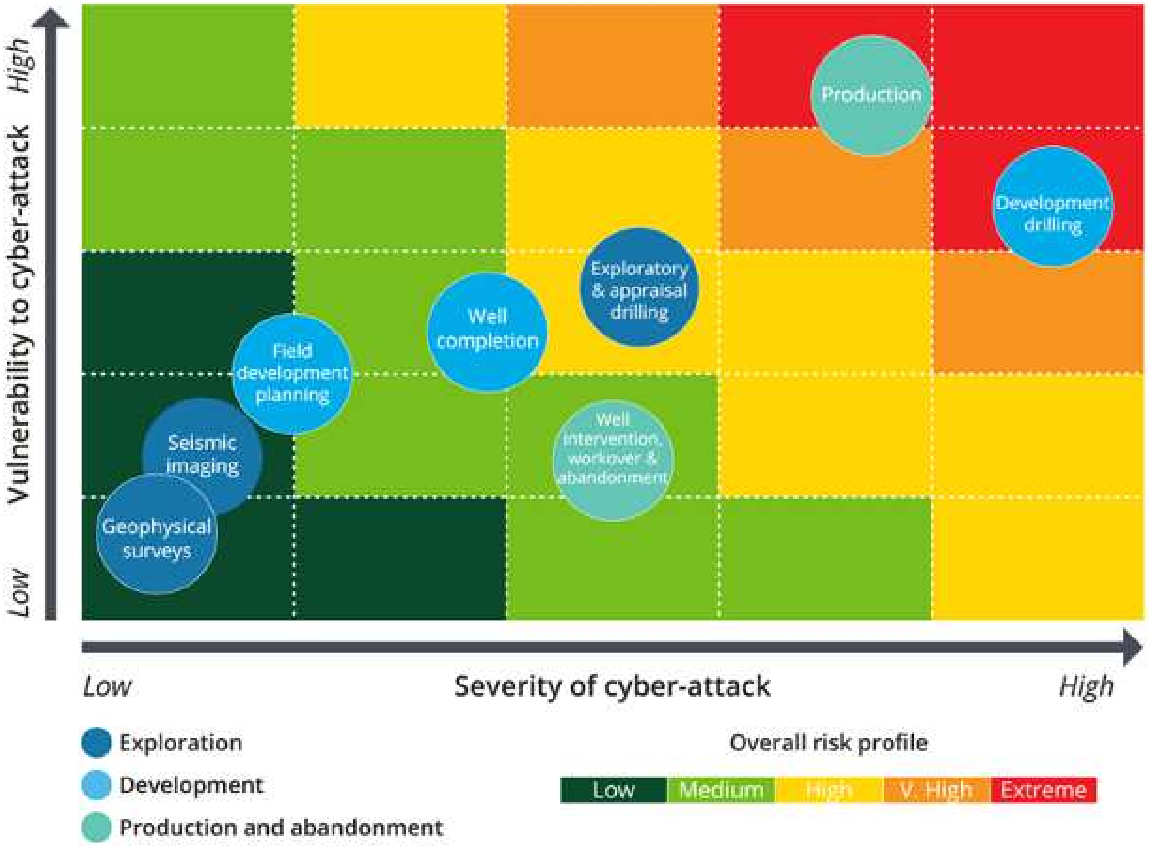


Figure 6 Cyber vulnerability by upstream operations [12].

International Journal of Trend in Scientific Research and Development ISSN: 2456-6470