PalArch's Journal of Archaeology of Egypt / Egyptology

DIGITAL TRANSFORMATION AND CYBER DISRUPTION IN THE OIL AND GAS INDUSTRY

Sayandeep Mandal[1], *Abhijit Chirputkar*[2]

Symbiosis Institute of Digital and Telecom Management,

Symbiosis International (Deemed University), Pune, India.

Email: chirputkar@sidtm.edu.in

Sayandeep Mandal, Abhijit Chirputkar: Digital Transformation and Cyber Disruption in the Oil and Gas Industry -- Palarch's Journal Of Archaeology Of Egypt/Egyptology 17(6). ISSN 1567-214x

Keywords: Digital Transformation, Operational technology, Cybersecurity.

ABSTRACT

Purpose: Digital transformation of Oil and Gas sector includes various types of technological changes in the industry and with these changes, various type of cyber threats also comes into the picture which is becoming a more serious concern for this industry. All the Industries are at the cusp of digital transformation, Oil and Gas sector is a very crucial sector, any potential damage by cyber threats will result in fall in market prices of oil severely.

Research Gap: This sector is behind many other industries in terms of digital transformation and cybersecurity. Proper mapping of digitization of Upstream, Midstream and downstream services with its cyber vulnerabilities is required.

Objective: The study focuses on the digital transformation and the cybersecurity of the Oil and Gas Industry.

Research methodology: The research methodology for this research is qualitative research, the study has been done by taking consideration of various peer-reviewed literature in the area of digital transformation and cybersecurity in the oil and gas sector.

Findings: After analyzing several research papers on cybersecurity, main cybersecurity threats have been identified and the framework has been proposed to mitigate the cyber risks

1. Introduction

Oil is known as black gold in today’s Industrial Revolution. 95 % of all the products which we use in our daily life is derived from Oil and Gas. We are also witnessing a major shift where Data now becomes the most important commodity. “Data is the New Oil” is the phrase of 22nd century. But for the Oil and Gas Industry, These datasets are the most crucial and confidential to sustain and remain profitable in Oil and Gas Business. This Industry generates an enormous amount of critical data every day, and it is becoming more vulnerable to potential attackers day by day Since this industry generates massive revenue and the whole world is depending on it. The reason behind producing enormous data is Digital transformation and its applications. This paper will be based on a qualitative approach to get a deep insight into the role of digital information and cybersecurity in highly competitive Oil and Gas Industry. Digital Transformation is becoming an essential part of every industry and along with it cyber threats are growing at an alarming rate. Oil and Gas industry is not behind in terms of digital transformation. In the last 2-3 years, this industry has started adapting many different digital solutions to enhance their production output, minimize their operating cost, and improving the decision taking time. Oil and Gas Companies are one of the most vulnerable to Cyber-attacks due to its criticality, These companies are the most critical in terms of their exploration, development and production. The study will help the Oil and Gas firms to analyse the potential vulnerabilities for a cyber-attack due to digital transformation.

2. Objective

This research paper deals with the digital transformation and cyber disruption happening in the Oil and Gas Industry. The objective is to know what type of digital technologies should be inculcated in this industry and how to cope up with the latest cyber threats. As every industry is using some kind of digital technologies in their domain, but in upcoming future, those who will able to harness these technologies with full potential will able to survive, and with digitisation, mapping of cyber vulnerabilities rising due to digitisation should be given the topmost priority in the field of research.

3. Literature Review

Digitization in Oil and Gas is playing an important role in fostering efficiency and effectiveness. According to the Consulting Firm McKinsey &Co , industry 4.0 can create a value equivalent to efficiency improvements of 15 to 20 per cent[1].This will produce more productive work rather than hard manual work.

Technology is the root word for Oil and Gas Sector nowadays, as this sector has to adapt various disruptive technologies because of the stiff international competition, falling of oil prices etc. The enablement of IoT has drastically cut down the costs and reduced the manpower. Considering Digital transformation as a vital part of this sector has also created a lot of apprehension in the part of cybersecurity. With each disruptive technology in oil and gas sector, a security vulnerability also gets created. The basic oil extraction process in Oil Rig follows, begins with a seismic survey of the site where the company wants to drill. "That is when the firm sends signals to the ground and bounces back so that they can locate places where oil and gas reside. After the company has identified a location, it starts drilling. Rigs are raised and rolled into place by a cantilever. After this connection of wells to pipelines is made that carry oil and gas to warehouses where the fluids-oil, gas and water are separated," First, the cargo is transported to a storage site before being shipped off to feed the fuel-thirsty industries.

The basic operation of an Oil & Gas firm can be classified as upstream, midstream and downstream.

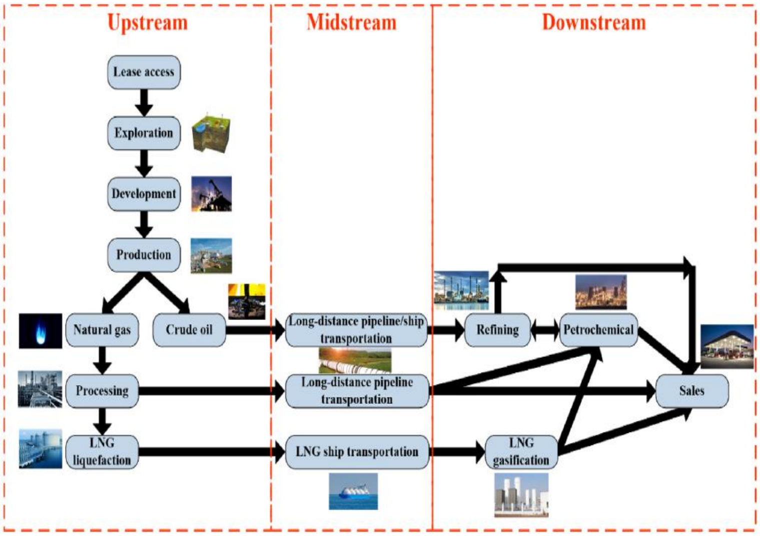


Fig :1 Oil and Gas Industry Workflow [2]

3.1 Digital transformation

It is the process of altering the things by using the latest technologies which will eventually help in the reduction of manual work and increase the effectiveness of production.[3]

A single drilling rig at an oil field can generate a massive amount of data, but only a small part of it used for the decision-making process. As other industries have progressed gradually in terms of digitization, now its high time for this sector to make a transformation.[3]

Digital transformation in this sector has many benefits, this transition will generate $1.6 trillion in value to the market, and environmental benefits include a reduction in CO2 emissions by nearly 1,300 million tones, savings of 800 million gallons of water.[3]

Secondly, after the digitization part, the most important one should be sought after is cyber threats.

In the past, OT (Operational Technology) networks were always separated from the internet, but considering the present need for efficiencies and real-time decision-making preclude that autonomy.

3.2 How Cyber Disruption can happen?

As per the definition given by Gartner "Operational technology (OT) is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events" [4]

A Cyberattack on an OT environment can have dangerous implications beyond financial losses which include environmental damage, outage of services and even most important threat would be on human life. There are well professionally qualified hackers who actively seek for some kind of exploitation in the security laps in an OT network, process control systems and critical infrastructure. There are many energy firms who have realized their key spending on security of their corporate IT systems but have overlooked the OT systems resulting to increase luring of cyber attackers to exploit some vulnerabilities in the OT system

OT applies to computer devices used to control manufacturing operations rather than administrative operations. Operational processes include production line management, supervision of mining activities, monitoring of oil and gas, etc. In these type of industries, these systems control the operations throughout the entire value chain, so they are the most critical part of the industry in terms of a cyber attack.[5]

Cybersecurity in the oil and gas field has several aspects. Risk-savvy security managers should base their investment decisions on a clear understanding of the essential business processes, the vulnerabilities of underlying technologies and the effect of infringements on the quality, integrity or confidentiality of process data. The availability and integrity of the process data from the extraction point or from the production end is the main aspect of security for field engineers. Any potential damage to the availability or integrity of process data will create a major problem.[5]

4. Research Methodology

The research methodology for this research is qualitative research, the study has been done by taking consideration of various peer-reviewed literature in the are of digital transformation and cybersecurity in the oil and gas sector. Most relevant articles were generated through keywords like cybersecurity, oil and gas, digital transformation. Papers have been collected from Scopus journal, Ebsco, Web of science, Frost and Sullivan and Google Scholar etc. The main reason for this study was to understand the growing importance of cyber safety measures that should take place with the growth of digital transformation.

As defined by Fink, "A literature review surveys books, scholarly articles, and any other sources relevant to a particular issue, area of research, or theory, and by so doing, provides a description, summary, and critical evaluation of these works with the research problem being investigated"[6] After searching various research article there were few single papers which combine the digital transformation and cybersecurity at once. So this paper covers the important aspects of digital transformation and the day by day rising cyber concerns.

In the following, this paper concludes the following topics:

1) Introduction- Provides the basic scenario importance of digital transformation and cyber disruptions.

2) Literature Review: Definition and importance of digital transformation and cybersecurity.

3) Research Methodology: It includes the type of research which has been conducted.

4) Findings of Research: Results and findings of reviewing various papers related to digital transformation and cybersecurity of oil and gas. Case study of some crucial ransomware attacks have covered in this research.

5) Security Recommendations: What are the key steps that Firms need to take to ensure complete cyber safety.

6) Managerial implication: How this paper will able to help to get some insights on digital transformation and cybersecurity.

7) Conclusion: Conclusion of the topic followed by the proposed framework.

5. Findings of the Research

Digital Transformation is not a cakewalk task for the firms. It varies from industry to industry, According to Digital maturity of the sector by McKinsey and Company 2018, Oil and Gas is at the very bottom line. The reason behind this is, producing an enormous amount of data is not the solution but producing and analysing the right quality of data is also important. With Right governance, structured data can be well optimised but when it comes for unstructured data like underground sounds, vibration, videos etc they are more challenging to gather and analyse. The second reason is the people around this industry, strong change management is needed. Progression towards digital transformation may be a slow-paced process in this type of industry but a structured process is required, people need to change their mindsets and companies should slowly start relying on the cloud, AI and robotics.[7]

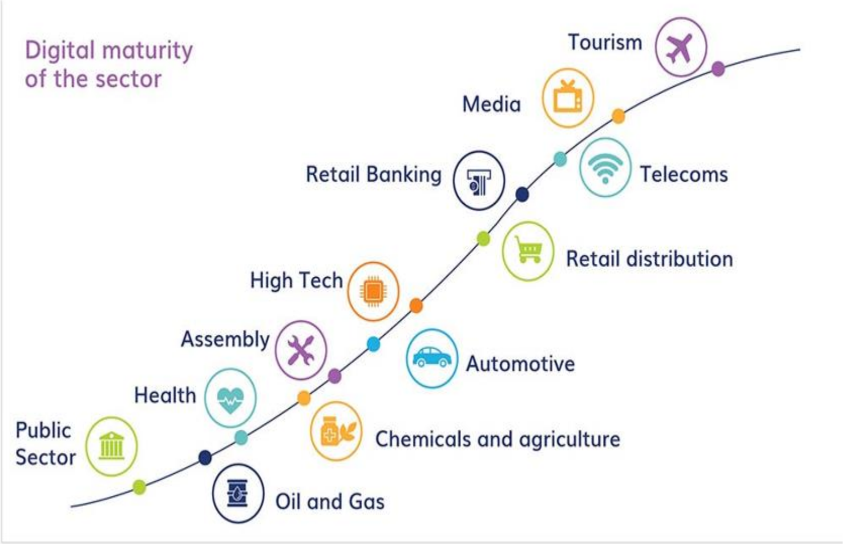


Fig 2: Digital Maturity of the sector, (McKinsey & Company 2018)

Digital maturity can be characterized as an awareness of the importance of technological technologies, as well as a solid, tech-oriented internal culture. Digitally mature organizations are data-driven, have a versatile IT structure and support and experience with technology at all levels of the enterprise.

5.1 Applications and opportunities for Digital transformation

The Oil and Gas Industry always has a large Capital expenditure, Operational expenditure and Health, safety and environment risk, therefore it is very crucial to monitor all the performance of the assets optimally as well as certified safety. This is the reason why oil and gas firms are using Industrial IoT solutions to track all the field equipment, analyse all the respective field data and make data-driven business decisions and applying control commands to optimize asset performance while reducing health, safety and environment risks.[8].

Since data is the new oil, With the adoption of the Internet of things, it enables a new concept called "brings data to experts to replace the traditional model of bringing the experts to the data".[9].

5.1.1 Applications of industrial IoT in Oil and Gas includes

Tank level monitoring, pipeline monitoring, leak detection, infrastructure monitoring, cargo shipping , carbon footprint control etc.

5.1.2 Predictive maintenance

Predictive maintenance is becoming one of the crucial technique in these firms, because Unexpected downtime has a very severe financial impact on Oil and Gas companies.

On average 1% annual unplanned downtime of a production facility (3.65 days) causes a loss of US$5.07 million[10]. There are generally three types of maintenance, i) Reactive maintenance,ii) preventive maintenance and iii) Predictive maintenance. In the case of reactive maintenance, the asset runs perfectly till it gets failed, after that repair time and substitution takes place. Preventive maintenance follows the OEM product specification sheet and includes repair and replacement at certain fixed interval periods. In predictive maintenance, collection of asset integrity and operation data takes place at a definite interval. The final collected data is analysed and after some applying algorithms, it gets processed and able to predict the status of the equipment.[11] . Predictive maintenance require sensors to collect data, IoT helps in this process by collecting the data and sending it to the servers. With the advent of 5G, these collected data from the sensor can be processed in Edge computing and will be able to deliver faster data-driven decisions.

With the growth of artificial intelligence predictive maintenance can be optimised far better.

5.1.3 Cloud Computing

As data is becoming a more critical asset for an organisation, how to process this data and get the best results out of it is the big question for everyone. Cloud computing is the only solution to store and analyse a large set of oil field data. With the advent of 5g, it will be very easy to achieve faster data throughputs without having significant infrastructure cost. Speed of fibre connectivity has finally reached to the offshore oil platforms, which will help in retrieval of data from the remote platforms.

The Cloud business is maturing very rapidly, platforms such as AWS, AZURE and GCP lead the market share. These companies made the infrastructure as a service more scalable.

Companies like BP and ExxonMobil have invested heavily on cloud platforms like AWS and Azure. The ultimate advantage of having cloud is i) Better use of Big Data is possible ii) More Agility iii) Reduction of on-premise infrastructure cost iv) Increase in security and v)increasing the efficiency.[12]

5.1.4 Digital Twin

Digital Twin creates the replica of the physical asset which will soon become an integral part of any type of industry. DT accelerate product and process development, optimise the performance and enable predictive maintenance.

Digital twin creates a replica model of production properties that can be continuously modified in real-time. This will create new prospects for asset management and a lot more. Digital twin's main goal is not to observe current situations, but rather to simulate operating parameters that have a major effect on the decision-making process. Example – British Petroleum (BP) is one of the companies that have invested in this technology and developed a highly advanced simulation and surveillance device called APEX. It will create replica versions of all of its production processes. With the help of APEX, the simulations that took 20-30 hours to complete will now be completed in 20 mins.

[13]

The most important part of this research is to understand the type of threats in this sector,

As per the Trend Micro Research[14], the types of threat are classified as follows:

5.2 Common types of Cyber-threats

As per the Trend Micro Research[14], the types of threat are classified as follows

5.2.1 Infrastructure Sabotage:

The attacker first needs to accumulate critical information about the target and then use this information to compromise systems or computer servers on the targeted network. The attacker does not need to maintain access to the system. The attacker may also try to destroy all the evidence of compromise while proceeding with the sabotage.

Sabotage in this context can be done via different actions:

□ Changing the behaviour of software

□ Deleting or wiping off specific content to disrupt the activity of the company

□ Deleting or wiping off as much content as possible on every accessible machine.

examples of these kinds of sabotage operations have been reported broadly, the most famous

being the Stuxnet case. Stuxnet was a piece of self-replicating malware that contained a very targeted and specific payload.

Another example is malware Industroyer.[15] This malware contains specific payloads for ICSs used in electric substations, although it can be refitted to target other types of critical infrastructure. In addition to these payloads, it contains a data wiper part that can be triggered to erase data and make systems unbootable.

The Shamoon campaigns, which had at least three known waves of attack from 2012 to 2018, on oil and gas companies have been incredibly aggressive. The biggest target of these attacks, a Saudi oil company, had about 30,000 computers rendered unbootable by the destructive malware. The impact was significant since a lot of the oil company's computer servers were disrupted for weeks. However, the world oil supply was essentially not affected by these attacks.[14]

5.2.2 Insider Attack

An insider — in most cases, a disgruntled employee seeking revenge or merely wanting to make easy money selling valuable data to competitors — can commit sabotage operations. Although there are several factors that can motivate a person to turn against their employer, revenge is the more dangerous type since the individual could not care less which part of the company is targeted. Blackmail can also be a motivation for an inside job.

An insider may do the following:

- Altering data to create problems, misuse access, or cause damage
- Deleting or destroying data from corporate servers, shared project folders, or any location the insider has access to.
- Stealing intellectual property for the insider's use or for a competitor's.
- Leaking sensitive corporate documents to third parties or competitors, or even uploading them to the internet.

Careful monitoring of user activity can bring this kind of activity to light, but the task is still very difficult. It might be difficult to distinguish the usual daily operations from sabotage actions — for example, simple actions like modifying a document or deleting a file could be part of a sabotage attempt.

5.2.3 Espionage and Data Theft

While sabotage of the daily operations is among the most damaging attacks on the oil and gas industry, data theft and espionage are important threats the industry needs to be aware of as well. As mentioned above, data theft and espionage can be the starting point of a larger destructive attack. Attackers often need specific information before attempting further action. Obtaining sensitive data like well drilling techniques, data on suspected oil and gas reserves, and special recipes for premium products can also translate to monetary gain for attackers.

5.2.4 DNS hijacking

DNS hijacking is a particularly dangerous attack used by a limited set of advanced attackers. The aim of DNS hijacking may include getting access to the corporate VPN network or corporate emails of governments and companies. This is particularly relevant for the oil industry, as we have seen a number of oil companies being targeted by advanced attackers who probably have certain geopolitical goals in mind.

Domain name System can serve as the platform for various types of attacks against corporate networks. DNS-based attacks on the corporate network is rising day by day.[16]

These are the two common ways in which DNS hijacking occurs:

1) "Man-in-the-Middle" attack: An intruder intercepts DNS requests from a user and deviates them to an attacker's own malicious Domain name system.

2) Attacks that use malware: an attacker infects a victim's machine via email or other malicious activity.

5.2.5 EVER-CHANGING MALWARE

In a targeted attack, specific viruses serve multiple purposes: intrusion, data theft, dissemination, and more. Keeping a foothold in a victim's network is important to a threat actor. They need to be able to send their malware continuously commands and to receive data. DNS tunnelling is a process by which the DNS protocol is used to transfer data between the malware and the controller. Both email and cloud services can be used as a means of communication.

5.2.6 Ransomware

In the past, cybercriminals spread ransomware everywhere they could, often using spam botnets to try and hack as many computers as possible. While it remains a serious threat to anyone who stores data on their device, ransomware has become an even greater threat as ransomware players target companies directly, with attacks that may have a major impact on day-to-day operations.

BitPaymer19 is one the dangerous ransomware family that targeted a U.S company specialised in oil well drilling services. Actors behind BitPaymer usually use spear phishing to infect their targets with initial malware before moving laterally and compromising the network further. They plan the ransomware in different locations and depending upon the absence of IT people i.e they can plan the ransomware on weekends and holidays.

5.3 Case study on Ransomware Attack

A famous target actor group APT33 is there which focuses on targeting the oil industry and its supply chains.

APT33 has shown particular interest in the aviation sector organizations active in both military and commercial capacities, as well as in the energy sector organizations with links to petrochemical production

APT33 has also affected European and Asian energy firms. A big oil firm with a presence in the U.K. and, in the fall of 2018, India had unique APT33 related infections. Few of the oil company's IP addresses interacted with the C&C timesync.com website, which hosted a Powerton C&C server from October to December 2018, then again in 2019.

In November and December 2019, a database server operated by a European oil company in India interacted with a Powerton C&C server used by APT33 for at least three weeks. It has been found that APT33 was possibly infiltrated by a major UK-based firm providing specialized services to oil refineries and petrochemical facilities in fall 2018.

APT33's best-known intrusion strategy was by emails using social engineering. It has been using the same type of lure for many years: a spear-phishing e-mail containing a work opening bid that may seem quite valid. Campaigns also targeted hiring process in the oil and aviation sectors.[14]

The email includes a path to the malicious .hta code. The.hta file may attempt to download a PowerShell script which can download additional APT33 malware to allow the group to stay in the target 's network.

Another cause of a Ransomware attack went with Mexican state-owned oil firm Premix, it was hit by a ransomware attack which halted their critical operation which prodded them to disconnect their network from the internet and back up their critical information from hard drives. As per the reports by Bloomberg, Premix servers were infected by Ryuk (a ransomware strain) that generally gets distribute via email phishing campaigns or botnets.[17]

Possible Solution: As per Cyware report, To proactively counter threats such as APT33, companies need advanced threats and behaviour-based malicious detection tools to identify and neutralize in real-time emerging IOCs and TTPs. In order to prevent these type of threats and develop shared strategies for countering these threats, companies must exchange strategic and tactical threats information with their trusted partners, ISACs and the regulatory bodies.

5.4 Recent Cyber-attacks in Oil and Gas industry

- Rosneft(June 2017)- Not Petya Ransomware attack
- Saudi Aramco (December 2017)- Triton malware attacked Triconex safety controllers shutting down some industrial processes.
- Energy Transfer Partner- EDI system was impacted.
- Saipem(December 2018)- Shamoon virus variant disabled roughly 300-400 servers and 100 workstations.

6. Security Recommendations for Oil and gas firms

Security of O&G firms is the most important part of the industry, as a small compromise in the supply chain can disrupt the entire market price. As proprietors and owners of One of the most important infrastructures for the country, Industry businesses take defence seriously With production and operational control systems (ICS) Technology (OT)-Electronic tracking and/or control Or physical asset monitoring-and avoidance Disruptions in the energy sector which can affect nationally Public safety and defence.[14]

As per the report by Defence in depth Cyberattacks on U.S. energy infrastructure are on the rise. The number of incidents reported Critical infrastructure goals rose from 245 With a comparable amount (290) in 2014 to 295 in 2015; In 2016. 1 Of the incidents recorded, roughly 20 One per cent (59 incidents reported) targeted the Power Business. [18]

Companies need to follow certain key steps to prevent any potential attack.

1) Performing data Integrity checks: Some critical data source like the data coming from an oil production site through sensors should be well digitally signed to prevent any kind of malicious attack.

2) Implementation of DNSSEC: Many oil and gas companies do not have Domain Name System Security Extensions (DNSSEC) implemented. DNSSEC means digitally signing DNS records of a domain name to a private key authoritative name server. DNSSEC helps fight DNS spoofing and hijacking.

3) Securing Business email: A firm should always be vigilant towards different types of mail, Firms should proactively use artificial intelligence in the regular business emails between their employees. Proper training should be given to the employees to identify spam emails properly.

4) Two-factor authentication is needed for Webmails:- DNS hijacking is easily possible for webmail. A well-planned Credential phishing attacks can take place easily in webmail, two-factor authentication and corporate VPN for webmail access should be there.

5) Proper Awareness Training for employees: It is one of the major issues all the energy firms generally face. Employees need to be trained properly to identify different types of cybersecurity issues. Proper SOPs should be there for any malicious attack

6) Enhancing Cloud Security: Digitisation of O&G firms leads to migrate their on-premise infrastructure to cloud, this will boost the company efficiency and reduces cost but the company sometimes forget to use the cloud security effectively.

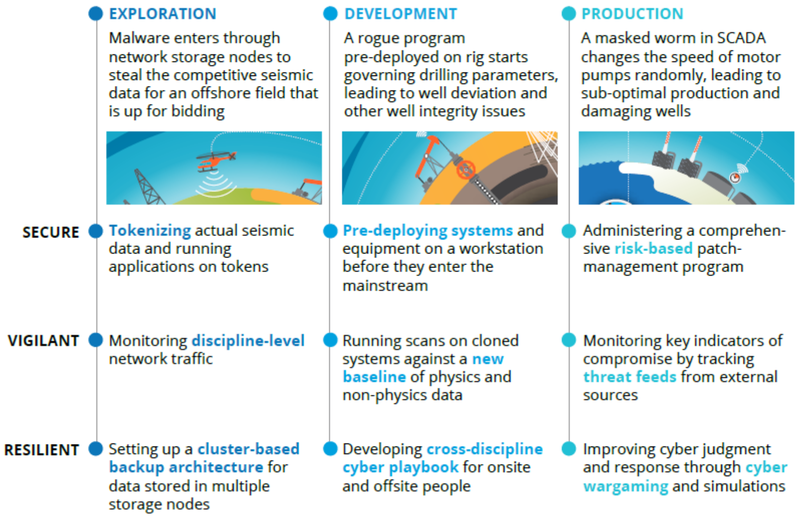
7) Defending against IoT and Botnets: Removing of unwanted protocols, ensuring the firmware is updated regularly and by segmenting IoT devices from the corporate network.

8) Segmentation of Network: Segmenting IoT devices from the corporate network is needed.

9) Software Updates: Office Software’s should be updated with latest security patch.

10) Storage units: The use of mobile devices and storage units should be monitored properly

As per the Deloitte Analysis Risk mitigation strategies for upstream operations are as follows:



	EXPLORATION	DEVELOPMENT	PRODUCTION
	Malware enters through network storage nodes to steal the competitive seismic data for an offshore field that is up for bidding	A rogue program pre-deployed on rig starts governing drilling parameters, leading to well deviation and other well integrity issues	A masked worm in SCADA changes the speed of motor pumps randomly, leading to sub-optimal production and damaging wells
SECURE	Tokenizing actual seismic data and running applications on tokens	Pre-deploying systems and equipment on a workstation before they enter the mainstream	Administering a comprehensive risk-based patch-management program
VIGILANT	Monitoring discipline-level network traffic	Running scans on cloned systems against a new baseline of physics and non-physics data	Monitoring key indicators of compromise by tracking threat feeds from external sources
RESILIENT	Setting up a cluster-based backup architecture for data stored in multiple storage nodes	Developing cross-discipline cyber playbook for onsite and offsite people	Improving cyber judgment and response through cyber wargaming and simulations

Fig 3: Cyber risk mitigation strategy,[19]

To implement a strong Cybersecurity Strategy, the most pivotal thing is to make a strong framework, The basic framework of cybersecurity is already given by NIST. Companies need to comply with this framework in order to achieve success.[19]

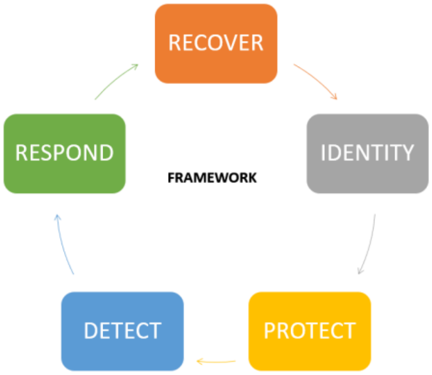


Fig 4: NIST FRAMEWORK(NIST 2018)

As per the IoT consortium and NIST industrial IoT framework, devices that depend on the IoT are particularly vulnerable as vendors are rushing to get products out in the marketplace without considering security elements.

7. Conclusion:

In this new age of connectivity, the past practices of isolation between the corporate and operation environment for oil and gas sectors have pretty much disappeared. As digitisation continues to grow in the operational environment and the risk of sophisticated cyber-attacks is increasing rapidly, the preparedness of industries is still in the initial phase.

Companies need to start building a proper digitisation model and simultaneously mapping each cyber vulnerability. The most important thing of Cybersecurity of a company is its cyber awareness training, employees are not used with the cyber threats training which creates a gap between their instincts and actual cyber knowledge.

Secondly, Companies can set up their dedicated cybersecurity team consisting of highly skilled ethical hackers. Segmentation of Operational technology network is one of the most important things to complete after digitisation, any malicious access to the operational network could create a disaster.

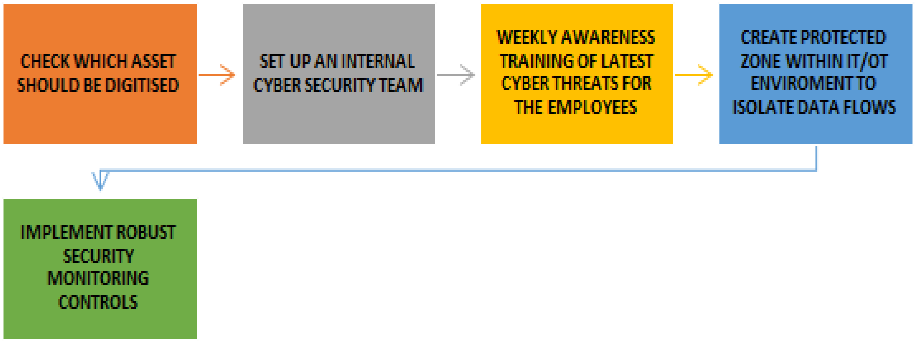

CHECK WHICH ASSET SHOULD BE DIGITISED
SET UP AN INTERNAL CYBER SECURITY TEAM
WEEKLY AWARENESS TRAINING OF LATEST CYBER THREATS FOR THE EMPLOYEES
CREATE PROTECTED ZONE WITHIN IT/OT ENVIROMENT TO ISOLATE DATA FLOWS
IMPLEMENT ROBUST SECURITY MONITORING CONTROLS

FIG 5: PROPOSED FRAMEWORK

8. Managerial Implication

The concept of this paper can benefit investors and industrialist in this field. Importance of digital transformation and the role of cybersecurity has been covered in this paper.

The companies which are inculcating digitisation in their domain, they can look forward to digital Twin and Edge Computing, as 5g is going to hit the market in the next couple of years. The major advantage will be for Business to Business deal, with the help of 5g Oil and Gas firms can foster their digitisation process in all the three sections i.e upstream, midstream and downstream and on the similar lines they also need to look into the cyber threats that may arrive with digital transformation. This paper covers some recent cyber-attacks and potential cyber threats in the oil and gas industry, which will help readers to get a better perspective about cyber threats. Companies need to prepare their cybersecurity framework according to their requirements because the upcoming future is all about data, and Oil and Gas sector generate sheer volume of data and protecting this crucial asset is very important.

References

O. Andreas, Behrendt; Nicolaiand, Christoph; Schmitz, Müller; Peter, “Industry 4.0 demystified--lean’s next level | McKinsey,” McKinsey & Company, 2017. https://www.mckinsey.com/business-functions/operations/our-insights/industry-4-0-demystified-leans-next-level (accessed Aug. 07, 2020).

H. Lu, L. Guo, M. Azimi, and K. Huang, “Oil and Gas 4.0 era: A systematic review and outlook,” Comput. Ind., vol. 111, pp. 68–90, 2019, doi: 10.1016/j.compind.2019.06.007.

World Economic Forum, “Digital Transformation Initiative: oil and gas industry whitepaper,” no. January, pp. 20–22, 2017.

“Definition of Operational Technology (OT) - Gartner Application Development and Platforms for Technical Professionals Glossary.” https://www.gartner.com/en/information-technology/glossary/operational-technology-ot (accessed Aug. 07, 2020).

P. Ciepiela, “Digitization and cyber disruption in oil and gas,” pp. 1–16, 2017.

A. Fink, “Conducting Research Literature Reviews: From the Internet to Paper - Arlene Fink - Google Books,” 2005. https://books.google.co.in/books?hl=en&lr=&id=0z1_DwAAQBAJ&oi=fnd&pg=PP1&dq=Fink,+Arlene.+Conducting+Research+Literature+Reviews&ots=14PriYVPhy&sig=p5Q6X0qTMhwKRpRn8oafyKBkobE&redir_esc=y#v=onepage&q=Fink%2C Arlene. Conducting Research Literature Reviews& (accessed Aug. 08, 2020).

U. Wagner, “Digital transformation and challenges,” Text. Netw., vol. 2018-May, no. 5–6, pp. 40–41, 2018.

O. Alsaadoun, “A cybersecurity prospective on industry 4.0: Enabler role of identity and access management,” Int. Pet. Technol. Conf. 2019, IPTC 2019, 2019, doi: 10.2523/iptc-19072-ms.

P. Zornio, “The control room is anywhere and everywhere: Putting the industrial internet of things to work offshore and beyond,” Proc. Annu. Offshore Technol. Conf., vol. 1, pp. 31–37, 2018, doi: 10.4043/28943-ms.

GE, “> DOWNTIME - The Impact of Digital on Unplanned Downtime,” pp. 3–4, 2016, [Online]. Available: https://www.bhge.com/sites/default/files/2017-12/impact-of-digital-on-unplanned-downtime-study.pdf.

T. R. Wanasinghe, R. G. Gosine, L. A. James, G. K. I. Mann, O. de Silva, and P. J. Warrian, “The Internet of Things in the Oil and Gas Industry: A Systematic Review,” IEEE Internet Things J., vol. XX, no. X, pp. 1–1, 2020, doi: 10.1109/jiot.2020.2995617.

S. O. Settemsdal and B. Bishop, “When to go with cloud or edge computing in offshore oil and gas,” Soc. Pet. Eng. - SPE Offshore Eur. Conf. Exhib. 2019, OE 2019, no. September, pp. 3–6, 2019, doi: 10.2118/195758-MS.

T. R. Wanasinghe et al., “Digital Twin for the Oil and Gas Industry: Overview, Research Trends, Opportunities, and Challenges,” IEEE Access, vol. 8, pp. 104175–104197, 2020, doi: 10.1109/ACCESS.2020.2998723.

F. Hacquebord and C. Pernet, “Drilling Deep A Look at Cyberattacks on the Oil and Gas Industry,” Drill. Deep A Look Cyberattacks Oil Gas Ind., pp. 1–35, 2019, [Online]. Available: https://www.trendmicro.com/vinfo/it/security/news/internet-of-things/drilling-deep-a-look-at-cyberattacks-on-the-oil-and-gas-industry.

“TROJ_INDUSTROYER.B - Threat Encyclopedia - Trend Micro PH.” https://www.trendmicro.com/vinfo/ph/threat-encyclopedia/malware/troj_industroyer.b (accessed Aug. 08, 2020).

V. C. Perta, M. V. Barbera, G. Tyson, H. Haddadi, and A. Mei, “A Glance through the VPN Looking Glass: IPv6 Leakage and DNS Hijacking in Commercial VPN clients,” Proc. Priv. Enhancing Technol., vol. 2015, no. 1, pp. 77–91, 2015, doi: 10.1515/popets-2015-0006.

A. Barrera, “Ransomware attack at Mexico’s Pemex halts work, threatens to cripple computers,” Reuters, 2019. https://uk.reuters.com/article/uk-mexico-pemex/ransomware-attack-at-mexicos-pemex-halts-work-threatens-to-cripple-computers-idUKKBN1XM045 (accessed Aug. 08, 2020).

Natural gas Council, “In the Natural Experiment,” pp. 121–130, 2015, doi: 10.1007/978-3-319-14403-0_7.

Anshu Mittal, Andrew Slaughter, and Paul Zonneveld, “Protecting the connected barrels - Cybersecurity for upstream oil and gas A report by Deloitte Center for Energy Solutions,” 2017.