DEVELOPMENT OF CYBERSECURITY MANDATE FOR INDIAN OIL AND GAS INDUSTRY

By

C.SUNDARARAMAN

SAP ID: 50001259

SCHOOL OF BUSINESS

submitted

IN PARTIAL FULFILMENT OF THE REQUIREMENT OF THE DEGREE OF DOCTOR OF PHILOSOPHY

to

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
DEHRADUN
June, 2018

Under the Guidance of

Internal Guide
Dr. Rajeev Srivastava
School of Business
UPES, Dehradun

Internal Co-guide
Dr. Ratna Banerjee
School of Business
UPES, Dehradun

External Guide
Dr. Swaminathan Mani
Tech Mahindra, Hyderabad

DEDICATED TO

JAYANTHI

ACKNOWLEDGEMENT

In my long journey of my research, I want to acknowledge people who helped me come throughout. First of all, I want to acknowledge my guide Dr.Rajeev Srivastava, to whom I turned to ever so often all the times. His quick turnaround responses always helped me. Also I need to thank my co-guide Dr.Ratna Banerjee, who gave technical inputs whenever needed. Both of them encouraged me to present my paper at the Doctoral colloquium at UPES. I am indebted to Dr.Swaminathan Mani, my colleague, my friend and an alumnus of UPES, who volunteered to extend his helping hand as my external guide. His continued support all through made a big difference. I am also very thankful to Dr.Krishnan Pandey, my ex-guide who always motivated me to continue my research journey. Without his motivation, I would have discontinued my research program, due to my persistent travel as part of my official work. My sincere gratitude to Dr.Pokriyal, who guided me on my research from both academic as well industry perspective. I would be very thankful to Ms.Rakhi Rual, Assistant Director (PhD Programs) who was promptly responding to my queries every time.

The voyage of discovery would not have been possible, but for the support from my family. My both parents have been in the academic circle all their life and they have been a keen inspiration for me to equip myself with my academic interest. My better-half Jayanthi has been instrumental in driving me to continue this journey. Whenever I lose momentum, she used to give the necessary stimulus. She even put up with my idiosyncrasies, even while we were on family vacations. Her help in proof-reading the report is immense. My two grown-up sons constantly encouraged me with their all kind of supports. Adithya used to take care of all my logistics needs, whenever I travel to Dehradun, so that I could focus on my research. Anirudh always used to give me a third person perspective on my research work. I would also like to thank my nephew Atulya, who helped me to do the second proof-reading of the report.

DECLARATION BY THE AUTHOR

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgement has been made in the text.

C. Sundararaman

June, 2018

THESIS COMPLETION CERTIFICATE

This is to certify that the thesis on "**Development of Cybersecurity Mandate for Indian Oil and Gas Industry"** by **C. Sundararaman** in partial completion of the requirements for the award of the Degree of the Doctor of Philosophy (Management) is an original work carried out by him under our joint supervision and guidance.

It is certified that the work has not been submitted else for the award of any other diploma or degree of this or any other university.

External Guide

Dr.Swaminathan Mani

Internal Guide	Co-Guide
Dr. Rajeev Srivastava	**Dr.Ratna Banerjee**

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS / ABBREVIATIONS

S.No	Acronym	Description
1	APT	Advanced Persistent Threats
2	AVE	Average Variance Extracted
3	B2B	Business to Business
4	BYOD	Bring Your Own Device
5	C2M2	Cyber-security Maturity Model
6	CAGR	Compound Annual Growth Rate
7	CIO	Chief Information Officer
8	CISO	Chief Information Security Officer
9	CERT	Computer Emergency Response Team
10	CFA	Confirmatory Factor Analysis
11	CII	Critical Information Infrastructure

S.No	**Acronym**	**Description**
12	CIIP	Critical Information Infrastructure Protection
13	CISP	Cybersecurity Information Sharing Partnership
14	CISO	Chief Information Security Officer
15	CIWIN	Critical Infrastruture Warning Information Network
16	COO	Chief Operating Officer
17	CPNI	Centre for Protection of National Infrastructure
18	DCS	Distributed Control System
19	DHS	Department of Homeland Security
20	DOE	Department of Energy
21	DOS	Denial of Service
22	DMZ	Demilitarized Zone
23	DSCI	Data Security Council of India

S.No	Acronym	Description
24	EECSP	Energy Expert Cyber Security Platform
25	EE-ISAC	European Energy Information Sharing Analysis Centre
26	EFA	Exploratory Factor Analysis
27	ENCS	European Network for Cyber Security
28	ENISA	European Network and Information Security Agency
29	EPC	Engineering, Procurement and Construction
30	EPCIP	European Program for Critical Infrastructure Protection
31	ERP	Enterprise Resource Planning
32	ETRM	Energy Trading and Risk Management
33	EUROSCSIE	European SCADA and Control Systems Information Exchange
34	FDI	Foreign Direct Investment

S.No	Acronym	Description
35	HELP	Hydrocarbon Exploration and Licensing Policy
36	HMI	Human Machine Interface
37	IADC	International Association of Drilling Contractos
38	ICS	Industrial Control System
39	ICT	Information and Communication Technology
40	IDSA	Institute of Defense and Analysis
41	IIoT	Industrial Internet of Things
42	INGAA	Interstate Natural Gas Association of America
43	IoT	Internet of Things
44	ISAC	Information Sharing and Collaboration
45	ISACs	Information Sharing and Analysis Centers
46	ISCD	Infrastructure Security Compliance Division

S.No	**Acronym**	**Description**
46	IT	Information Technology
47	IT IS-EUC	Incident and Threat Information Sharing EU Centre
48	KMO	Kaiser Meyer Olkin
49	LAN	Local Area Network
50	MES	Manufacturing Execution System
51	MIS	Management Information System
52	MTOE	Million Tons of Oil Equivalent
53	NCI	National Critical Infrastructure
54	NCII	National Critical Information Infrastructure
55	NCIIPC	National Critical Information Infrastructure Protection Centre
56	NCP	National Cybersecurity Policy
57	NELP	New Exploration Licensing Policy

S.No	**Acronym**	**Description**
58	NDMA	National Disaster Management Authority
59	NIST	National Institute of Standards and Technology (US)
60	NCSC	National Cyber Security Centre
61	NTRO	National Technical Research Organization
62	OT	Operational Technology
63	PCS	Process Control System
64	PMO	Prime Minsiter’s Office
65	PSC	Production Sharing Contract
66	RMSEA	Root Mean Square Error of Approximation
67	RO	Research Objective
68	RQ	Research Question
69	RTO	Remote Terminal Unit

S.No	**Acronym**	**Description**
70	SCADA	Supervisory Control and Data Acquisition
71	SEM	Structured Equation Modeling
72	Sl-CERT	Slovenian Computer Emergency Response Team
73	SOP	Standard Operating Procesure
74	SRA	Security Risk Assesment
75	TNCEIP	Thematic Network on Critical Energy Infrastruture Protection
76	WAN	Wide Area Network

WORKING DEFINITIONS OF VARIABLES

S.No	Variable	Working Definition
1	**Baseline cybersecurity risk assessment**	Conduct a baseline cybersecurity risk assessment and arrive at a risk score.
2	**Periodic Cybersecurity Drills**	Periodic Industry wide cybersecurity drills to be conducted in the Oil and Gas industry.
3	**Third Party Security Assessment**	Third party security assessments to be made mandatory on an annual basis in the Oil and Gas industry.
4	**Cybersecurity Assessment Review**	Cybersecurity risk assessments to be reviewed periodically.
5	**Inventory Cyber-physical assets**	Organization to identify and maintain an inventory of its critical cyber-physical assets.
6	**Certification of Products**	There is a need to enforce security certifications of products, which are categorized as critical cyber-physical assets.

7	**Logging of Changes in Cyber-physical Assets**	Every changes to the cyber-physical assets to be logged.
8	**Identity Management**	Ascertaining and taking care of identities to provision and de-provision of identities to entities. (removing identities when someone quits the organization)
9	**Credentials Management**	Periodic review of the credentials to ensure that they are connected with the correct person or entity.
10	**Revoking Access**	Access to cyber physical assets to be revoked when no longer required.
11	**Collect Information from Industry Association**	Collection of useful information for threat identification and response from dependable sources like Industry Associations, CERT etc
12	**Analyzing Vulnerability Information**	Collection and analyzing of vulnerability information for minimizing cybersecurity vulnerabilities by using scanning tools, penetration tests, and cybersecurity tests.
13	**Threat and Vulnerability Management**	Stakeholders to be identified and involved for threat and vulnerability management activities.

14	**Collab Forum for Sharing**	Need to set up an Oil and Gas industry specific collaboration forum to share security knowledge, incidents and best practices**.**
15	**Disclosure to Nodal Agency**	Disclosure of breaches and security incidents to a nodal agency to be made mandatory for companies in the Oil and Gas industry.
16	**Directory at Nodal Agency**	Importance of having a nodal agency to maintain a current directory of industry wide cybersecurity emergency response contacts.
17	**Responsible Senior Executive**	Organization to identify and nominate a senior executive (like Chief Information Security Officer - CISO) who would be reporting to the Board.
18	**Mandatory Education & Training**	Cybersecurity education and training to be made mandatory for all employees in the Oil and Gas industry.
19	**Employee Screening**	Employees working in or having access to sensitive domains to be screened and security cleared.

20	**Cybersecurity Program Strategy**	Cybersecurity program strategy to incorporate a list of cybersecurity goals and a plan to meet them.
21	**Executive Sponsorship**	Sponsorship is important for implementing the cybersecurity program for providing resources like People, Tools and Funding.

1 EXECUTIVE SUMMARY

Today is the era of Information technology, which made an outstanding and constructive influence on the society. With the arrival of internet, the development and the power of the connected world have beaten anything else in the history of the human race. As we embark on the journey of digital transformation, the thin line between the real world and the virtual are merging impeccably. The digital world would intensify our reliance on the connected infrastructure. Nation's critical infrastructure like banking, energy, telecom, transport and health among others have a massive reliance towards the IT infrastructure. Though the IT infrastructure carries so much of advantages and benefits, it has got its own challenges.

Today, any nation can be easily be brought down, by a mere cyber-attack on its critical infrastructure. There are solid evidences for such attacks in the past on the critical infrastructure of a nation. For example the Stuxnet and Shamoon kind of attacks have revealed that cyber-attacks could trigger substantial harm and be a hazard to National Critical Infrastructure. It is because of this reason, the protection of National Critical Infrastructure has become a topic, when world leaders meet and discuss. That's why, even whenever the Prime Minister of our country, Mr.Narendra Modi visits abroad, cybersecurity happens to be in most of the foreign policy interventions, more than any other subject.

As on date many of the nation states have sufficiently responded by framing the requisite cyber-security policy, guidelines and regulations to protect the National Critical Infrastructures. Countries such as the US, UK and India have a documented cybersecurity policy and have articulated their strategy to shielding the nation's critical information infrastructure. While the cyber threats and attacks have spanned across a number of domains, the energy sector has been particularly targeted. Close to half off all the attacks have been focused on the energy sector alone. The US and EU also have a domain specific cybersecurity regulation or guidelines for the Oil and Gas industry.

In India, like any other country, the oil and gas industry performs a crucial position in deciding the important divisions of the economy. Energy demand drives a chief role towards the economic progerss in India and so the oil and gas' need is likely to raise, thereby this sector favorable for investment. Several new policies were put forth by The Government of India to meet the increasing demand. Today cent percent Foreign Direct Investment (FDI) has been allowed by our government in many segments of the petroleum industry like Exploration & Production, Refining & Marketing. Because of this initiative today we are able to draw the much needed domestic and foreign investment which would set a different pace for the industry.

By the year 2040, India's oil demand will mature at a CAGR of 3.6% to 458 Million Tons of Oil Equivalent (MTOE) as per Mr.Dharmendra Pradhan, Minister of State for Petroleum and Natural Gas. This is because the economy is likely to proliferate beyond five times than its current magnitude.

As we see the mega investments happening in the oil and gas sector, the companies are equally focusing on building ICT capability in the facilities. Everywhere there is digital transformation journey happening today. In IT enabled intervention and digitalization, in spite of many positives that have come about as part of the automation, the flipside is that there would be increased threat exposure from cyber vulnerabilities. Cybersecurity planning plays a vital role. If there is a lack in cybersecurity planning, the IT infrastructure especially while the assets are IOT enabled, will see a shake or downfall in the country's Oil and Gas industry's stability. The ideal solution is to mandate a domain specific cybersecurity policy for the Oil and Gas industry in India which is absent today.

This research study is focused on understanding the cybersecurity challenges in the Indian Oil and Gas industry and to identify the significant constituents of the cybersecurity policy and in turn, to enhance the security position of the sector. The extensive literature review carried out as part of the research study was focused on

- Understanding the impact of cyber threats to NCI with specific reference to the Oil and Gas industry.
- Studying the impact of cyber threats in the Indian context.
- Studying the methodology and the regulatory intervention taken up by the developed countries such as US and EU to improve the security position in the Oil and Gas industry.
- Identifying the variables that form the building blocks of the cybersecurity policy for the Oil and Gas industry.
- Identifying the theoretical constructs

The survey of the literature demonstrated that there are minor literature on the cybersecurity challenges in the Indian Oil and Gas industry and an absence of domain specific regulations for the Indian Oil and Gas industry. Further review of theoretical constructs in cybersecurity showed that that there is no equivalent of the Laudon and Trever's 4 layer E-commerce security model in the cybersecurity domain. The research problem, objectives and questions is a continuum of the literature gaps.

The research study was executed in two stage using Mixed Methods' research. To start with Qualitative Research was leveraged strategy to identify the cybersecurity challenges in the Oil and Gas industry. Later by using Quantitative methods the factors that can enhance the cybersecurity in the Indian Oil and Gas sector were identified. The literature review and global experience served as the input to building the interview protocol that was used to conduct a semi-structured interview with respondents.

The purposive sample of respondents for the in-depth interview were drawn from the Government, industry and academia. The interviews were then transcribed and analyzed by adapting to Ritchie's and Spencer's Framework Analysis. Atlas TI software was used for coding and analysis. The outcome of the in-depth interview answered the first research question and the gist was captured in the next steps.

The digital transformation as well the IT-OT integration happening in the Oil and Gas industry is delivering a number of benefits. However there is very little appreciation of the risks or exposure to cybersecurity threats which come along with the increased adoption of IT both among all levels at the petroleum sector. A majority of the organization don’t have the designated CXO level executive responsible for the cybersecurity and the security function is usually managed within the IT organization. Given the diversity and the financial status of the players in the Indian Oil and Gas industry, a principle based regulatory intervention emerged as a preferred choice to enhance cybersecurity in the petroleum sector. The in-depth interview also helped narrow down the focus list of 21 variables that were relevant to the Indian Oil and Gas industry. These variables were the input to the Likert-type scale for the second stage of quantitative analysis.

The questionnaire built on 5-point Likert scale was administered to 306 respondents after confirming the reliability and validity. The research used Exploratory Factor Analysis (EFA) to identify the initial set of four factors and then established their significance with a Confirmatory Factor Analysis (CFA).

Four factors viz. Identity and Access Mgmt., Risk Mgmt, Asset, Change and Configuration Mgmt.and Information Sharing and Collaboration emerged as significant factors from the Confirmatory Factor Analysis. These four factors are the recommended constituents of the domain specific cybersecurity mandate for the Indian Petroleum sector.

The recommendations proposed to Indian Petroleum sector industry are explained as follows:-

i. Mandatory Oil and Gas Sector-specific Cybersecurity Guidelines

The Ministry of Petroleum and Natural Gas should formulate mandatory Oil and Gas sector-specific cybersecurity guidelines. To start with, the mandatory guidelines can be principle focused i.e. at a high level rather than specific guidelines. But at a later stage it should also start addressing the different sub-businesses of the streams, since the impacts due to cybersecurity incident vary for different business processes of the industry. Hence specific guidelines for Exploration and Production in Upstream segment, Energy Trading and Risk Management (ETRM), Pipelines, Shipping in Midstream segment and Refining and Retail Marketing in Downstream segment can be thought of.

ii. Responsible Senior Person as Cybersecurity Custodian

The role of information technology in the Oil and Gas industry has undergone a sea-change in the past two decades. Also with the arrival of Internet of Things (IoT) technology and the concepts of digital transformation in the coming days, the role of IT would be significant. Hence, it is vital for the Indian oil and gas industry to have the senior executive roles such as Chief Information Security Officer (CISO). In fact, if the company is has an integrated operations i.e. having presence in multiple chains, they can think of having individual CISOs for every segment of the value chain. The individual CISOs can report to a Group CISO, who may be treated on par with the Directors. This way the accountability and responsibility towards cybersecurity can be enhanced.

iii. Workforce Management

When the impact due to cybersecurity incident would be going higher and higher in the coming days, there is need for a security-awareness culture across the organization at all levels. Though the detailed and periodic training is mandatory for the IT group, the other groups should also be exposed to the basic training modules on cybersecurity. This essential as each one of them handle vital data and information, whose breach can make a huge impact on the business. The organization should also bring in compulsory background screening and vetting of the employees, before they are on-boarded.

iv. Critical Cyber-Physical Asset Protection

Security certifications are required for critical cyber-physical assets. Organizations should identify, maintain a baseline their critical cyber-physical assets. These assets should be subject to period security audits. This step would become essential as organizations would start encouraging its employees to adopt the concept of "Bring Your OW Devices" (BYOD). The role of IoT devices in the industry would make the certification and periodical assessment of the cyber-physical assets a mandatory one.

v. Information Sharing and Collaboration

In the USA, ONG-ISAC is a central pool of cyber threat information for the O&G industry. It takes care of different segments of the Oil and Gas value chain from cyber threats by timely sharing of the cyber intelligence. This body offers a platform for members to share the cyber intelligence information between its members. In Europe, there exists an initiative called, "The Thematic Network on Critical Energy Infrastructure Protection" (TNCEIP). The initiative of the European Commission is to bring together the European owners and operators in the electricity, gas and oil sectors. Members of this program periodically exchange information related to cyber incidents.

In India, a similar organization specifically catering to the cybersecurity needs of the Oil and Gas industry is yet to evolve. The government should take necessary measures to set up a critical incident response team and define the process to react to a cyber-emergency. The ministry should facilitate the setup of a forum for the players in the Oil and Gas industry and promote information sharing and collaboration including disclosure of cybersecurity incidents. Information Sharing and Communication policy makers need to focus on

- Setting up a nodal agency maintaining current directory of industry wide cybersecurity emergency response contacts.
- A mechanism for the disclosure of breaches and security incidents in Oil and Gas industry to the nodal agency.

- Collecting useful information from reliable sources like Industry Associations, CERT etc.
- Work with industry specific collaboration forum to share security knowledge, incidents and best practices.

The ISAC nodal body can be a new setup similar to Computer Emergency Response Team (CERT), which was formed in the Indian Power Sector in the recent years.

vi. Security Audits

Oil and Gas industry should start conducting self-assessments for evaluating their cybersecurity posture, which shall be followed by periodic third party security audits. This can be similar to the Cybersecurity Capability Maturity Model (C2M2) framework that is being used in the oil and gas industry in the United States. Regulatory body should facilitate Industry wide security drills to prepare the organizations to handle a real life cybersecurity incident. In the Oil and Gas industry, IT implementation and the plant automation are there for so long. With the arrival of the IoT devices, the industry should quickly go towards larger adoption of IT and digital transformation. In this context, security assessments and audits would enhance the cybersecurity to a great extent.

vii. Collaboration with Academic Institutions

There are few reputed academic institutions like University of Petroleum and Energy Studies (UPES), Dehradun, Pundit Dindayal Petroleum University (PDPU), Gandhinagar, Rajiv Gandhi Institute of Petroleum Technology, Rae Bareli offering multitude of courses in the Oil and Gas segment. Since the industry cannot afford to have too many people in their Cybersecurity team, the industry can collaborate with the above institutions in the following areas with respect to cybersecurity:-

- Knowledge sharing
- Reverse knowledge sharing
- Tri-party arrangements

- Policy formulation & Updating

In this research, the researcher has identified the components for the cybersecurity mandate in the Indian Oil and Gas sector. The research helped zeroed in four major elements that would contribute to augment the security aspects in the Indian Oil and Gas industry. The 4 factors are:-

1. Identity & Access Mgmt.
2. Risk Mgmt.
3. Asset, Change and Configuration Mgmt.
4. Information Sharing and Collaboration

In the e-Commerce industry, Laudon and Trever suggested a 4-layer cybersecurity model. Data Protection, Technology, Organization Policies and Procedures with Laws & Industry standards forming the model. All the 4 layers are relevant to the Oil and Gas industry as well. However the oil and gas industry brings with it "industry-specific Information Sharing and Collaboration", which does not have relevance in the e-commerce industry. The contribution to theory from this research is the extension of the Laudon and Trever's 4 layer e-commerce security model by including the "Industry-specific Information Sharing and Collaboration" regarding the Oil and Gas industry's cybersecurity. The contribution to theory from this theory is the extension of Laudon and Trever's 4 layer e-commerce security model by including "Information Sharing and Collaboration", regarding the cybersecurity aspects of the Oil and Gas industry.

2 INTRODUCTION

2.1 OVERVIEW

Today every enterprise is subject to greater cybercrime vulnerabilities due to increasing complexity in Information Technology. Oil and Gas industry cannot take any exception and they need to cope with the ongoing cyber threats. In the digital era, organizations are increasingly relying on digital technologies to do business, and hence exposed to cyber threats more than ever. With the integration of the IT system and OT system, today cybercrime can take many structures, extending from cyber spying to attempts to destabilize company's physical operations, causing in physical destruction to causality. Today O&G companies have become more vulnerable to cyber threats as their operations have become more digital involving mobile, cloud and sensor technologies.

Critical business or physical operations in an Oil and Gas industry can be disrupted by attacks on networks. Lack of testing SCADA components, lack of awareness to information sensitivity can be ascribed to the major threats. Inappropriate encryption techniques can make the issues complex. O&G companies are subject to recurring and most of the times successful attempts by vested interests to access their long term strategic plans, exploration and production details and business negotiation details. Hackers were also effective in pilfering O&G Company's manuals, guide, standard operating procedures and the most vital geological information.

2.2 BUSINESS PROBLEM

In view of the huge implications and increasing probability of above risks, the Government of India (GOI) came out with policies and procedures issued by the National Critical Information Infrastructure Protection Centre (NCIIPC). These policies and procedures are anticipated to take all essential activities to enable guard the Critical Information Infrastructure (CII). But now with the advent of IT/OT integration, the Oil and Gas industry is under great threat. The generic cybersecurity policies may not be enough to address the threats other than the traditional threats. However in India, sector-specific policies are also yet to be defined.

The business problem can be summarized as:

"Deficient cybersecurity in the Indian Oil and Gas sector threatens business growth, economy and national security". This paper attempts to analyze the constituents of the domain specific cybersecurity mandate for the Indian oil and gas industry.

2.3 RATIONALE & MOTIVATION

Until 2013 India had no cybersecurity policy. Due to the pressure exerted by various agencies, the Government of India came out with its **National Cybersecurity Policy 2013** on 2 July 2013. Department of Information Technology (DIT) announced the creation of a dedicated body to guard India's Critical Information Infrastructure (CIIs) in 2014.

Regrettably there seem to have been few measures have been taken to establish the mandate of the government's announcement since 2014. For the Oil and Gas industry, specific preventive actions are yet to be planned and limited information on this is available in the public domain. Though the government of India has already formulated the **Indian Computer Emergency Response Team (CERT-In)** to address the cybersecurity threat and initiate steps to avoid repetition of the same, to the Oil and Gas industry of the country from cyber threats are seldom available which is a cause of concern.

In this context, identifying constituents of the domain specific cybersecurity mandate for Indian oil and gas industry is the need of the hour.

2.4 OUTLINE OF THE STUDY

The research and objectives were met by the research strategy of this study. Qualitative as well Quantitative research strategies were done. Mixed methods was leveraged for this research. In-depth interview was conducted and Qualitative research strategy and analysis was done on its outcome. This helped to address the first question and also to understand more on the challenges in cybersecurity in the Oil and Gas industry. Quantitative Research strategy, which followed helped to determine the constituents of cybersecurity mandate in the Oil and Gas industry. To determine the factors and establish their significance, This study used both Exploratory Factor Analysis (EFA) and Confirmatory Factor Analysis (CFA).

2.5 CONTRIBUTION OF THE STUDY

There is two-fold approach out of this research contribution. The cybersecurity challenges in the Indian Oil and Gas industry were identified as well its determining factors helped to enhance the cybersecurity posture in the Indian Oil and Gas industry. This research contributed to the existing theoretical construct or body of knowledge by enhancing and adopting 4 layer Laudon and Trever security model for the Oil and Gas industry.

2.6 ORGANIZATION OF THE REPORT

The following sections give an account of the research study.

Chapter 1: Executive Summary. The executive summary gives a quick synopsis of the thesis.

Chapter 2: Introduction. An introduction to the research study is provided in this chapter. The issues and challenges in the cybersecurity domain are highlighted. This chapter provides a holistic view of the entire research.

Chapter 3: Literature Review. The prevailing body of knowledge in this domain is summarized in this literature review. Specifically the cyber-security extortions to the national infrastructure and the Oil and Gas industry is identified through this literature review. It establishes the necessity for a regulatory intervention to enhance the cybersecurity posture. The review also focuses the domain specific cybersecurity regulations and mandates for the Oil and Gas industry in the advanced countries. Through the literature review, the research gaps were established the initial set of variables that would enhance the cybersecurity posture were identified.

Chapter 4: Research Design. This chapter on research design gives an outline for the complete research study. It discussed about the research viewpoint and the selection of research strategy with the reasons of the choices made. This chapter deliberated the research problem, the research objectives, the research questions and the approach to formation of scales, reliability and validity testing and approach to data collection.

Chapter 5: Data Analysis and Interpretation. The implementation of the road map planned out in the research design is primarily covered in this chapter. It gives an emphasis on the qualitative and quantitative research techniques used to answer the research questions. It features the approach to qualitative data analysis using Framework Analysis to analyze the in-depth interviews, using Atlas-TI software. The second section of the chapter narrates the quantitative data analysis to answer the Research Question 2 (RQ2), which were resolved using the IBM SPSS and Amos tool sets.

Chapter 6: Conclusion and Recommendations. This chapter summarizes the recommendations for enhancing the cybersecurity in the Indian Oil and Gas industry, limitations of the study and opportunities for future research.

Chapter 7: Appendix: The last segment of the research is the Appendices, which include the interview protocol used, the detailed questionnaire that was used for data gathering, references & bibliography and the profile of the author.

2.7 CONCLUDING REMARKS

After conventional domains such as sea, air and space, battle has now entered the fifth domain called cyberspace. A nation's security and comfort and economic progress is interwoven with its critical infrastructure. Contrasting the physical world, where the government is accountable for protecting the nation's boundaries, in the cyber world the ownership and the responsibility are not just limited to government alone. It would be the combined responsibility of the government sector, private sector, relevant bodies and the individual citizen. The nation's cybersecurity policy is the apex document that weaves together the individual responsibilities to form a cohesive and strong defense.

Next to the power sector, the Oil and Gas industry is the heart beat that enables the functioning of the remaining critical infrastructure sectors and is also the one that faces the lop-sided mainstream attacks. The Indian Oil and Gas industry, while it is overwhelmed with a number of challenges, has been investing in automation and expanding in the digital space. While automation and digitalization are a crucial investment, security requirements outlay would be a major requisite for its sustained accomplishment. A domain specific cybersecurity policy will serve to enhance the security posture of the organizations in this sector. The research recognized the challenges in the Indian Oil and Gas industry and the factors that would enhance the cyber posture of the organizations in the Oil and Gas industry. It is believed that this research will contribute in a minor scale in making a cyber-safe nation.

3 LITERATURE REVIEW

3.1 OVERVIEW

The intention of the literature review is to recognize the prevailing body of knowledge in a territory. This literature review addresses the impact of cyber threats to National Critical Infrastructure (NCI) across the globe and in India, with specific emphasis on the Oil & Gas Industry. The review also discusses the regulatory intervention adapted by the U.S and U.K to improve the security position of their national critical infrastructure in general as well the Oil & Gas industry. The review also pursues to study the theoretical concepts in the cybersecurity domain. Last but not the least, it also identifies the gaps in the literature that would become the basis or the foundation for the research problem.

3.2 INTRODUCTION

The literature review is the beginning a research journey and is an endeavor to recognize the prevailing body of knowledge in the territory of interest.

The purposes of a review are listed below, (Chris Hart, 1998), w.r.t the objectives:-

- What has been completed and what is pending
- Identifying the vital variables, pertinent to the topic
- Understanding the subject and its structure
- Producing and achieving a new perspective
- Instituting the context of the problem

Cooper's Taxonomy of Literature Review provides the framework to plan and approach a literature review. (Cooper, H. M, 1988). Cooper recommends that the literature review be classified according to the features and groupings as shown in Table 3.1.

Table 3-1 Taxonomy of Literature Reviews by Cooper

(Source - Cooper, 1988)

Features	**Groupings**
Focus	Research Methods, Research Outcome, Theories, Practice or Applications
Goal	Integration, Disapproval, Identification of core issues
Perspective	Neutral Representation or Adoption of Position
Coverage	Exhaustive, Pivotal or Central, Representative, Exhaustive with Selective Citation
Organization	Historical, Conceptual, Methodological
Audience	Scholars, Practitioners or Policy Makers, General public

The core aspect of this literature review include:

- To study the impact of cyber susceptibilities and threats to the National Critical Infrastructure not only in a particular region but across the globe

- To study the impact of cyber susceptibilities and threats to the Oil and Gas industry
- To study the approach and regulatory intervention adopted by US and UK to enhance the security posture of National Critical Infrastructure in general and in specific Oil & Gas industry
- To identify the list of variables that shape the core building block of the cybersecurity policy for the Oil & Gas industry in a country
- To study the theoretical constructs in the cybersecurity domain
- To identify the gaps in the literature / research

3.3 SOURCE OF LITERATURE

The primary source of articles were from peer reviewed journals and publications in Science Direct, EBSCO, Elsevier and similar sources, publications from government agencies including the CERT-In, US NIST, US Government Accountability Office (GAO), UK CPNI and other global agencies like ENISA and research work carried out by think-tanks and industrial bodies like Institute of Defense Strategy and Analysis (IDSA) and Data Security Council of India (DSCI) amongst others. The focus was on the experience in the U.S and the U.K as these countries have been the pioneer in the domain of cybersecurity and India shares a similar judicial and bureaucratic structure with the United Kingdom. The following Table 3.2 depicts the details of the same:

Table 3-2 Reports and Databases Referred to and Keywords Being Used

Keywords used	**Reports Published by**	**Databases**
Cybersecurity Data Breach	McKinsey Morgan Stanley	Elsevier

Cyber Attack DCS SCADA FCS RTU PCN ICS IT/OT Integration DMZ Critical Infrastructure Vulnerability Information Security ERP	Deloitte Gartner Forrester IDC Ernst & Young Accenture Microsoft Annual Reports of Indian Oil & Gas Companies Cybersecurity policy of Govt. of India ACM -Symposium on Information, Computer & Communication Security Computer Standards & Interfaces Computers & Security Engineering Science and Technology, an International Journal	Taylor & Francis Google-scholar EBSCO JSTOR

	IEEE International Conference on Industrial Informatics IEEE International Conferences on Internet of Things IFAC-Papers Online International Journal of Critical Infrastructure Protection	

3.4 LITERATURE REVIEW UNDER THEMES

There are 9 themes that arose from Literature Review, directing to the Research Gaps and heading to the need for Research is mentioned in the appendix. The table mapping the literature review against the themes are available in the appendix.

3.5 DETAILED LITERATURE REVIEW

3.5.1 NATIONAL CRITICAL INFRASTRUCTURE

- "Infrastructure is defined as the basic physical and organizational structures and facilities. (ScienceDaily). Common roads, buildings, day to day power supplies required for the functioning of a society/enterprise are few of those."
- PDD-63 (The United States Presidential Decision Directives - 63, 1998) under the aegis of President Bill Clinton, is perceived as a policy document that positioned the necessity for protecting the Critical Infrastructure. Critical infrastructure is described as the vital physical and computer related systems for the least operations of the economy and government. The Directive identified 16 sectors in both the

government and private domains as critical to the wellbeing of the nation. Energy, Telecommunication, Banking & Finance System (BFS), Transportation and emergency services are few among these.

- In the US, the Department of Homeland Security (DHS) is the nodal agency for the safety and security of the Critical Infrastructure. The DHS considers cyber systems as the nerve systems and the governance system of the country.
- UK follows a similar approach and describes national infrastructure as the facilities, systems, and networks essential for providing the vital services & the functioning of the country. The Centre for Protection of National Infrastructure lists around 13 sectors that form a part of National Infrastructure in UK. (CPNI, 2018) The Cabinet office is the apex body which is accountable for the Cybersecurity. UK ascertains cyber as a Tier One risk as part of its National Security Strategy and calls out cyberattacks by other nation states, terrorists or organized crime as a priority area to be addressed.
- According to the National Technical Research Organization (NTRO), which is a technical agency under the PMO, Critical Information Infrastructure is described as "computer resources, the breakdown or destruction of which, shall have serious impact on national security, economy, public health or safety". (R.K.Sharma, 2016). The Department of Electronics and Information Technology, as part of its Critical Information Infrastructure policy document says that Defense, Finance, Energy, Transport and Telecommunication service as part of critical infrastructure in India. (The Gazette of India, Ministry of Electronics & Information Technology, 2014).

3.5.2 NATIONAL CRITICAL INFRASTRUCTURE UNDER THREAT

According to a global survey of technology executives, Kim Zetter says that the repeated cyberattacks target only the critical infrastructure systems around the world. (Zetter, 2010). It is believed that cyber-attacks are initiated by the terrorists and foreign nation states & not just only from individual cybercriminals. The range of the attacks vary from:

- DNS poisoning
- SQL injection attacks
- Large scale rejection of service attacks
- Silent efforts to penetrate networks undetected
- Malware corruption.

Aim of these criminals is not only to shut down of the services or operations but also include theft of services and data or extortion.

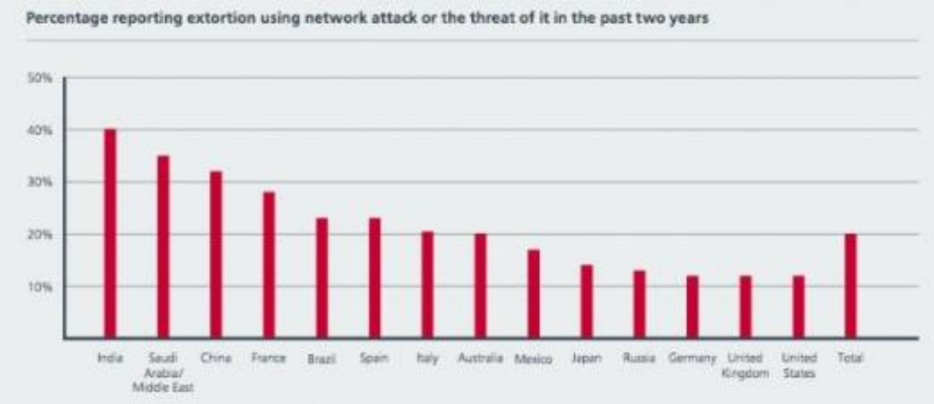


Figure 3-1 Percentage Reporting Extortions

20% of the participants of the survey said they were the targets of extortion or blackmailing by cyberattack in the last two years. Extortion or blackmailing was found to be more prevalent in countries like India, the Middle East, China and France and uncommon among the developed countries like U.S. and U.K. (Zetter, 2010).

- According to Kroger, in today's world National Critical Infrastructure (NCI) is the use of modern information technology to integrate smaller systems into larger ones. (Kroger, 2008). There is widespread usage of Commercial off the Shelf products (COTS) and changes in the operating settings that have reduced the operating margins in systems that are core to NCI. (Kroger, 2008).

- Onyeji, Ijeoma, et al. says that in the Oil and Gas industry, the ICT systems are heavily integrated with the other and thereby making the whole system susceptible for cyber-attacks. (Onyeji, Ijeoma, et al, 2014). They also add that that the one of the ways to tackle the cyber issue is by integrating the best practices, frequent knowledge-sharing sessions, periodical training and effective use of tools. (Onyeji, Ijeoma, et al, 2014).

- Sharma.M in his monograph highlights that the modern societies and economies rest on few of the basic services like banking, electricity, transportation & communication. (Sharma, M, 2017). If the state has to function seamlessly then these critical infrastructures should also function well. He adds, the latest progress in this space have identified a new aspect of security attaching to primary vulnerabilities or exposures and interdependencies. (Sharma, M, 2017).

Table 3-3 Critical Infrastructure Sectors in India

Transportation	**Power & Energy**	**Information & Communication Technology**	**Banking, Financial Services and Insurance**	**E-Governance & Strategic Public Enterprises**
Civil Aviation Railways Shipping	Thermal Power Hydraulic Power	PSTN Network Satellite Communication Network Backbone	Reserve Bank of India Stock Exchanges	NIC E-Governance Infrastructure

	Nuclear Power Petroleum / Natural Gas Power Grid Refineries	Mobile Telephony Broadcasting	Banking Clearing Houses Payment Gateways	

Nation-states, terror outfits and crime organizations have various purposes to manipulate the vulnerabilities in the diverse levels of cyber architecture. (Sharma, M, 2017). Though every country has the paramount technology, practices and policies on cybersecurity, it is still a challenge to safe guard all the vital elements of infrastructures.

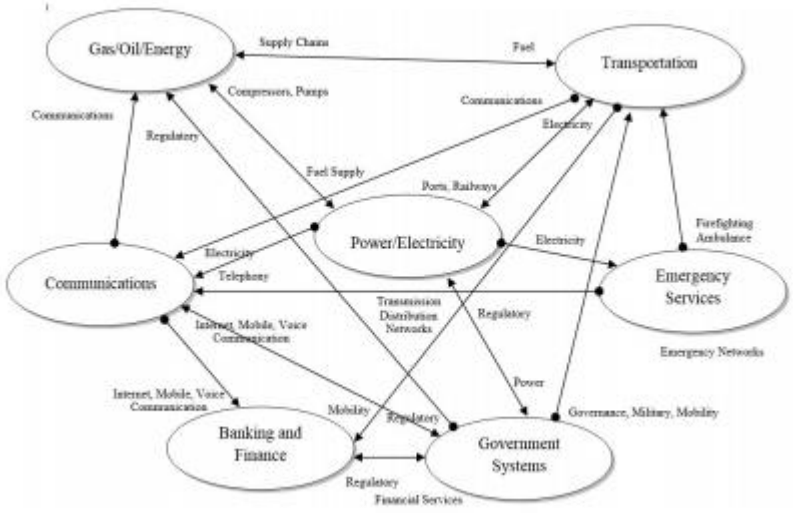


Figure 3-2 Interdependency among Critical Sectors

Source: By Sharma.M with inputs from http://www.rbtxllc.com/energy-industry.html (Sharma, M, 2017)

All the critical sectors, such as transportation, communications and government services, depend upon the power/electricity sector for their basic requirement of electricity supply, which powers the railways, airports and communication systems such as switching centers or telephone exchanges. In an interdependent function, the power/ electricity sector itself depends on transportation for fuel supplies and communications for its data transmission or to maintain health of the transmission/distribution networks. Similarly, governments depend on the banking and financial services for all monetary needs. The banking sector is technology driven, and communications sector plays a pivotal role in seamless banking operations. (Sharma, M, 2017).

- Ryu et al. show the issues faced by the current Process Control System (PCS) security which illustrates the need for improvement and lists favorable areas of research in PCS security. (Ryu et al., 2009). In the energy sector, the implementation of Process Control System (PCS) and the Supervisory Control & Data Acquisition (SCADA) system help remotely monitoring and controlling the process plants. (Ryu et al., 2009).
- Tai et al, says that the critical infrastructures lead to the formation of highly interlocked networks (Tai Kizhakkedath et al., 2013) These networks are interdependent and anytime, any failure in the network can have a cascading impact on HSE aspacts and the economy. One way is to identify possible unanticipated inter dependencies among infrastructure mechanisms that can cause risky interruptions on failure in some part of the network. (Tai Kizhakkedath et al., 2013).
- While innovation brings with it significant benefits, Hellstorm.T in his work brings out how disruptive innovations also serves to increase the vulnerabilities in the NCI. (Tomas Hellstrom, 2006). The author builds on the “pressure and release” (PAR) model to discuss the dynamics of vulnerabilities and brings out how the inter-dependencies in the systems has meant that a weakness or unsafe condition in one of the players negatively impacts the rest. (Tomas Hellstrom, 2006).

- Modern day NCI is managed and controlled by ICS. Nicholson, et al., highlight the growing sprawl of SCADA systems across various domains and therefore the extensive destruction that can be caused by an outbreak on the SCADA systems to NCI. (Nicholson Webber et al., 2012). There is sufficient literature to establish that NCI is susceptible to cybersecurity attacks and modern day smart infrastructure serves to provide a larger threat landscape that increases the vulnerabilities. (Nicholson Webber et al., 2012).

3.5.3 CYBER THREATS IN THE OIL & GAS INDUSTRY

- Transparency Market Research studies the global market for oil & gas cybersecurity by factoring in various crucial aspects and generates a report. Both historical & current data was taken to gauge the size of the market. In order to extrapolate the future market trajectory, it throws some information on the limits and growth drivers. (Transparency Market Research, 2016). In addition, in order to probe the current leading players and their strategies, the report also influences the market-leading analytical tools. To counter various threats, cybersecurity systems are implemented in oil & gas operational sites. Few common threats are: Misuse by people working Inside, various crime ware, cyber spying, attack on web application attacks are to name a few common Oil & Gas cyber-attack threats. (Transparency Market Research, 2016).
- Cybersecurity systems supervises all the critical processes during plant shutdown and helps to disclose the utilities interruption, undetected spills, and other installation terrorism. If there is an effective cybersecurity systems in place, then we are ensured of seamless operations right from exploration and production of Oil & Gas to their delivery to end-users. (Transparency Market Research, 2016). The global market for Oil & Gas cybersecurity can be split broadly into physical security and network security. (Transparency Market Research, 2016). The three major segments, sector-wise, which are seen can be grouped into upstream sector, midstream cybersecurity sector, and downstream sector. (Transparency Market Research, 2016).

- **Upstream sector cybersecurity challenges** **(**Transparency Market Research, 2016).

  When we look into the upstream sector cybersecurity challenges, they are:
  Breach of confidential information or data pertaining to:

  - Drilling operations
  - Planned endeavors
  - Production sharing contracts (PSC)
  - Block figures
  - Tenders
  - Information from field production
  - Drilling methodologies.

- **Midstream Oil & Gas sector** (Transparency Market Research, 2016).

  When we look into the Cyber-threats in the midstream Oil & Gas sector is mostly related to:

  - Supply chain logistics
  - Distribution networks
  - Storage information
  - Pipeline data
  - Pipeline & transportation information

- **Downstream sector cybersecurity challengesu** (Transparency Market Research, 2016).

  In the downstream, major cyber-security challenges pertain to:

  - Information regarding the refinery
  - Data of consumers
  - Distribution to the final user
  - Data pertaining to the retailer
  - Industrial plants & manufacturing data.

From the above challenges we find that the Upstream is most prone area for cyber-attacks. (Transparency Market Research, 2016).

- Viewing from the geographic standpoint, Europe & North America are potential markets for Oil & Gas cybersecurity. They take all possible steps & invest heavily in sophisticated cybersecurity systems to ensure that there are no breaches. Regarding the Shale gas development & production, U.S. & Canada take every small stop to ensure cybersecurity. In order to safeguard operational processes in the entire Oil & Gas industry, Europe and North America take lot of security steps. These continents in order to improve their revenues are trying their best to tap into the China and India markets in Asia Pacific. (Transparency Market Research, 2016).
- Accenture in their report on "Reducing Industrial Cyber Risk in Oil & Gas" suggests just 3 simple steps that Oil & Gas companies can adopt to lower the amount of industrial cyber risk. (Accenture, 2016). A simple way for companies to lower the amount of industrial cyber risk is to check their employees and other humans involved in the large operation. (Accenture, 2016). Any major cybersecurity strategy focuses heavily on human behaviors. Oil & Gas companies invest time and money in general cybersecurity education for their employees, but this is not always the case for industrial cybersecurity, so this is a good beginning. (Accenture, 2016). A different way is by basing your corporate strategy on a recognized industry standard or framework. Other organizations have invested significantly in their development, so use them to your advantage. The final step is to ensure that your enterprise IT and operational IT organizations are aligned. (Accenture, 2016). While this is a difficult task, any industrial cybersecurity program is set to fail if the two teams are not strategically aligned. These two groups often have competing agendas and objectives. The goal of enterprise IT is to adopt innovative technologies to improve data security and accessibility; operational technology intends to keep assets and legacy infrastructure running by maintaining existing technology and adding tried-and-tested products. (Accenture, 2016). However, failing to address either one's

concerns could lead to low adoption and possible failure. Three ways that Oil & Gas companies can address industrial cybersecurity concern are: investing in employee's education, choosing a standard, and aligning the IT organizations. (Accenture, 2016).

- Also Accenture in one of their reports on "Handling Cyber-attack in Energy Networks" suggests simple ways that Oil & Gas companies can make big improvements in industrial cybersecurity. (Accenture, 2016). One way to begin is to fund education for employees by teaching them about general cybersecurity. (Accenture, 2016). It also helps to select a recognized industry standard for cybersecurity, like the National Institute of Standards and Technology (NIST) cybersecurity charter in the US. This charter allows for companies to measure their progress, test resiliency and develop strategies for cyber defense and recovery. (Accenture, 2016).

- Accenture in their report on "Outside the Box - Protecting Core Operations" says that although Oil & Gas executives express confidence in their cybersecurity strategies overall, 60 % still view cyberattacks as a bit of a black box. (Accenture, 2017). Accenture highlights that as the mandate to protect Oil & Gas core operations goes critical, cracking open the black box would be imperative. (Accenture, 2017).

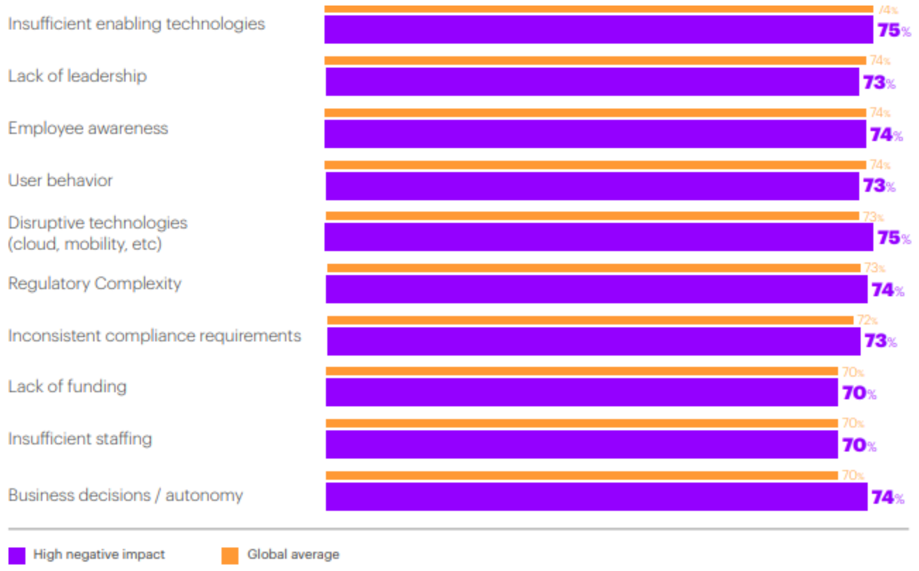


Figure 3-3 Factors Adversely Affecting Compliance

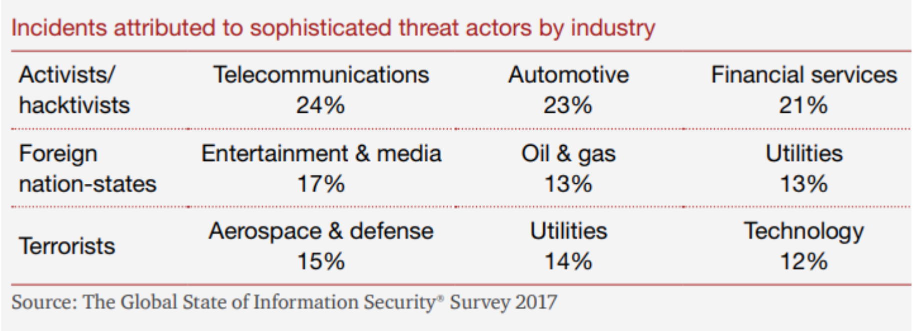
Source - Outside the Box - Protecting Core Operations - Accenture

- In addition, the successful completion of compliance program goals can be confused by companies with the actions necessary to prevent the business from breaches. The lack of transparency within compliance programs themselves may contribute to the problem. For example, when asked which factors negatively affect compliance, 70 % to 75 % of energy executives gave all the listed factors the same highly negative ratings – indicating a failure to prioritize factors that pose the greatest risk. (Accenture, 2017).

- DNV GL in a study identifies the top 10 persistent cybersecurity susceptible issues for the Norwegian offshore companies. (DNV GL, 2015). Though the study was dedicated to the Norwegian operations, the concerns are also valid to the Oil and Gas operations across the globe. The top 10 cybersecurity vulnerabilities are: (DNV GL, 2015)
  - Poor awareness on cybersecurity among employees
  - Insufficient cybersecurity culture between various stakeholders
  - Operations done from remote manner
  - Lack of improvement in IT products with known vulnerabilities

    - Inadequate isolation of data networks
    - Rampant use of mobile technology with various devices
    - Networks connecting onshore and offshore facilities
    - Poorly secured data rooms, cabinets, etc.
    - Software susceptible for breaches
    - Obsolete control systems
- Pricewaterhouse Coopers (PWC) in their report on “Embedding cybersecurity into the energy ecosystem” sums up how the energy companies with effective security approaches are focusing on 3 main areas: (Price Waterhouse Coopers (PWC), 2013).
    - Giving high priority for corporate resources and defending valuable things
    - Employing proactive cybersecurity practices, so that the business is enable to focus on the business rather than addressing the reactive measures
    - Well-organized association with strategy creators and regulatory authorities so that they are ready to respond on any eventuality

The key findings of Pricewaterhouse Coopers’s (PWC) Global State of Information Security Survey 2017 reveal that businesses in all industries are vulnerable to geopolitical threats. (Price Waterhouse Coopers (PWC), 2017).



Incidents attributed to sophisticated threat actors by industry

Activists/ hacktivists	Telecommunications 24%	Automotive 23%	Financial services 21%
Foreign nation-states	Entertainment & media 17%	Oil & gas 13%	Utilities 13%
Terrorists	Aerospace & defense 15%	Utilities 14%	Technology 12%

Source: The Global State of Information Security® Survey 2017

Figure 3-4 Incidents Attributed to Threat Actors by Industry

Today every business or every industry has become vulnerable to geopolitical threats. When comparing Oil & Gas with other industries, nation-state incidents are highest in the entertainment and Oil & Gas industries. (Price Waterhouse Coopers (PWC), 2017).

- RiskWatch International says that companies in the petroleum sector face a growing number of security challenges. (RiskWatch, 2012) The companies' private security is forced to combat external and internal, new strategy and tactics of opponents. The forces face issues from extremists (both national and foreign) as well as criminal organizations, cybersecurity breaches and disgruntled employees. RiskWatch advises the approach of addition of security personnel in the early phase of the Oil & Gas industry projects i.e. in the planning phase itself for better-coordinated and more cost effective approach to security. (RiskWatch, 2012).
- Candid Wueest in the Symantec research report says that today the energy segment is a key target for cyber-attacks. (Candid Wueest, 2014). Cyber-attacks have become a regular phenomenon, with innumerable threats endeavoring to advance a position even in the well protected organizations. (Candid Wueest, 2014). Approximately every day, 5 directed attacks are happening in the energy sector. Day by day, these attacks are becoming progressively complex (Candid Wueest, 2014). Energy sector has become the second highest sector with 16% of the attacks in the last six months in 2012. (Candid Wueest, 2014). This was primarily because of a massive attack against a specific oil and gas major. Survey reveal that the energy sector was placed 5th position with 7.6 % of all the cyber in the first six months in 2013. It was witnesses that attackers have become very effective and start concentrating on minor tasks that does not get noticed. (Candid Wueest, 2014). The attackers incline to look for specific information such as maps and seismic data of potential fields which are highly valuable. (Candid Wueest, 2014). Attacks similar to the previously occurred frequently result in huge monetary damages. These attacks are most likely orchestrated by government mercenaries, adversaries, internal attackers or hacktivists. (Candid Wueest, 2014). Chris Dalby looks growth of the cyber insurance market in the Oil & Gas industry and how it is becoming an essential part of a company's coverage. (Chris Dalby, 2016).

- The insurance industry has been somewhat slow to respond to the new need for its oil clients. (Chris Dalby (2016). Current outdated policies cover data loss or IT downtime. However, the policies fail to cover the physical harm or monetary loss. (Chris Dalby (2016).
- Christopher Bronk et al, gives a detailed account of the Shamoon virus attach on Saudi Aramco facilities. On Aug 15, 2002, Saudi Aramco was hit by a computer virus that perhaps would have propagated through the network and affected nearly 30,000 personal computers. (Christopher Bronk, E. T. R, 2013). As per the press reports, it could have taken up to 2 weeks to reinstate the network and return to normal business. Following this commotion, the impact include loss of data and disabled workstations, the loss of which were not quantified. (Christopher Bronk, E. T. R, 2013).

- Iii Robb et al. views that implementation of Security Vulnerability Assessment (SVA) programs are essential components of an all-inclusive risk management program. This is again vital for a strong and efficient security program for the corporates. (Iii Robb, et al., 2006). After 9-11, SVAs have been extensively implemented by many industry sectors including the oil and gas. (Iii Robb, et al., 2006). SVAs will permit the Oil & Gas industry to carry on to enhance its security posture and confirm to the progressively changing rigorous security centered regulations. (Iii Robb, et al., 2006).

- In 2017, Economic Times CISO carried an article mentioned that many enterprise are dearth of appropriate cyber analytics technology to monitor the breaches and attacks especially the Oil and Gas companies in this domain. (Economic Times CISO, Accenture, 2017). According to Accenture, many of them are not entirely sure how or when cyberattacks might occur and harm their business. (Economic Times CISO, Accenture, 2017). In the High Performance Security 2016 Report conducted by Accenture, a major segment of the Oil and Gas Company leaders surveyed (74% of 186 leaders) have agreed that cybersecurity measures would yield valuable outcome. (Economic Times CISO, Accenture, 2017). In fact, many of them (>75%) believe their key strategies would be able to prevent service interruptions as well safeguard their companies' valuable information and reputations. Conversely, roughly 60 % of energy leaders do not understand the functionality or timings of the cyberattacks. Additionally, the energy sector leaders were doubtful than their counter parts in other industries with respect to the ability to measure the severity of breaches and frequency of cybersecurity breaches. (Economic Times CISO, Accenture, 2017)

- Elbaradie, stresses that networks and the cyber systems must actively protect the Industrial Control System from cyber-attacks, against a variety of eventuality. (Elbaradie, M, 2017). His presentation was to provide an insight to participants on how to strengthen the defensive posture of their organization. The presentation also covered critical controls to mitigate targeted cyber intrusions to ICS. (Elbaradie, M, 2017).
    - Inventory of cyber-physical assets
    - Secure configuration for HW/SW systems
    - Malware Defense
    - Capability to recover data
    - Gap assessment on security skills suitable training programs
    - Controlled use of administrative rights
    - Boundary defense
    - Audit systems
    - Patch Management

- Tripwire Report conducted by Dimensional Research in November 2015, 82% of Oil & Gas industry participants have agreed that their organizations registered an upsurge in successful cyber-attacks over one year. (Tripwire, 2016). 53% of them have said the cyberattacks have increased between 50-100% over the past month of the survey period. 69% of them have said they were not confident their companies would be able to identify all the cyberattacks. (Tripwire, 2016)

- International Association of Drilling Contractors (IADC)'s ART Cybersecurity Subcommittee issued "IADC Guidelines for Assessing and Managing Cybersecurity Risks to Drilling Assets" Other guidelines under development: (International Association of Drilling Contractors, IADC, 2018).
    - Guidelines for Minimum Cybersecurity Requirements for Drilling Assets
    - Guidelines for Network Segmentation
    - Cybersecurity training – Training employees, with a focus on managing and accessing risks
    - Guidelines for strengthening control systems focusing on existing drilling assets (to include patching)
    - Guidelines for security monitoring and audit
- Prasenj Saha says that Oil and Gas companies should plan and execute sophisticated monitoring systems that are backed up by an efficient risk management system in order to alleviate the risks of cyber-attacks. (Prasenj Saha, 2018). The framework shall be flexible enough to accommodate changes that include diverse technologies. (Prasenj Saha, 2018).

- Muhammad Ali Nasir et al.mentions that the energy sector aggressively considers into cyber risk assessment across the globe, since this has a cascading effect. Any risk at any stage in the supply chain would have an impact on rest of the segments. In addition to harming function operations within an organization, Cyber-attacks also damage a company's well standing with shareholders and reputation overall which adversely affects finances. (Muhammad Ali Nasir et al., 2015). Organizations that are more willing to secure assets and information are more capable when it comes to responding quickly and accurately to cyber incidents and prevail longer than organizations who are not. In response, a modular plan was advised to lessen the cyber risks in global supply chain. (Muhammad Ali Nasir et al., 2015). The goal was to identify possible threats at every step and recommend immediate counter measures.

The authors have also tabulated the most likely threats feasible in the global oil supply chain. They also highlighted immediate measures. (Muhammad Ali Nasir et al., 2015). The possible cyber-attacks in the Oil & Gas Supply Chain are listed in Table 3--4

Table 3-4 Possible Cyber-attacks in the Oil Supply Chain

(Source – (Muhammad Ali Nasir et al., 2015)

Department	**Possible threats**	**Possible Measures**
Exploration	Information seepage Inference attacks Insider Information	Policy on Access Control Monitoring of Facilities Training of personnel on Security
Production	Infiltration by infested devices Breach of valuable information	Separation of Internal network Vs Internet Ban usage of memory cards or hard drives Effective reporting
Pipelines	False information ruining pipelines	Secure communication architecture Secure broadcasting
Shipping	Falsification of information on Geo Position Product distortion False or No reporting of anomaly	Securing GPS information Usage of RFID tags Thwarting fake tags Log monitoring for intrusion attempts Training Employee

Storage	Poor communication system Distorted database Distorted logs	Invasion recognition Security event analysis Safe dissemination Control of Inventory
Retain Marketing & B2B Marketing	Illegitimate data mining Fraudalant mailers Illeagal access Distortion of information	Evaluation plan for 3rd parties Antivirus software Firewalls Access based on roles and responsibilities

- Tim Haidar says that cybersecurity inside the Oil and Gas industry is a menace that is being overlooked many a times. It can create massive monetary repercussion as well fatality in worst case. (Tim Haidar, 2015). The US ICS-CERT has identified trends and have listed an increasing number of attacks on the Industrial Control systems. (Tim Haidar, 2015). Moreover, it notes that:
    - In the U.S, 53% of cyber-attacks target primarily the energy sector
    - Protective mechanisms do not trap 30% of malware
    - Advanced Persistent Threats (APT) contribute 55% of the attacks

- According to Corporate Citizenship Report of Exxonmobil, at ExxonMobil, the malicious actions increased fivefold from 2013-2014 (30,000 malicious actions to 150,000). (ExxonMobil, 2010).

- The Willis Energy Market Review, 2014 reports that 40% of all the attacks on the critical infrastructure in the US were targeted at the Energy Sector and goes on to identify that Cyber risk has been reported as part of the Top 10 global business risk for the first time in history, the Allianz "Risk Barometer" survey for the year 2014 (Willis, 2014).

- Aarab, N et al. describes a process for developing security policy and requirements based on internationally recognized industry standards and tailored for control and automation systems. (Najoua Aarab, Siv Hilde Houmb, Kent Hulick, & Erlend A. Engum, 2014).

- National Cybersecurity and Communications Integration Center (ICSCERT) at US answered to 295 incidents related to cybersecurity in 2015. (Department of Homeland Security, NCCIC, & ICS-CERT, 2015). This means a 20% upsurge over 2014. Among all the sectors, the Energy sector stood second with 46 incidents. (Department of Homeland Security, NCCIC, & ICS-CERT, 2015).

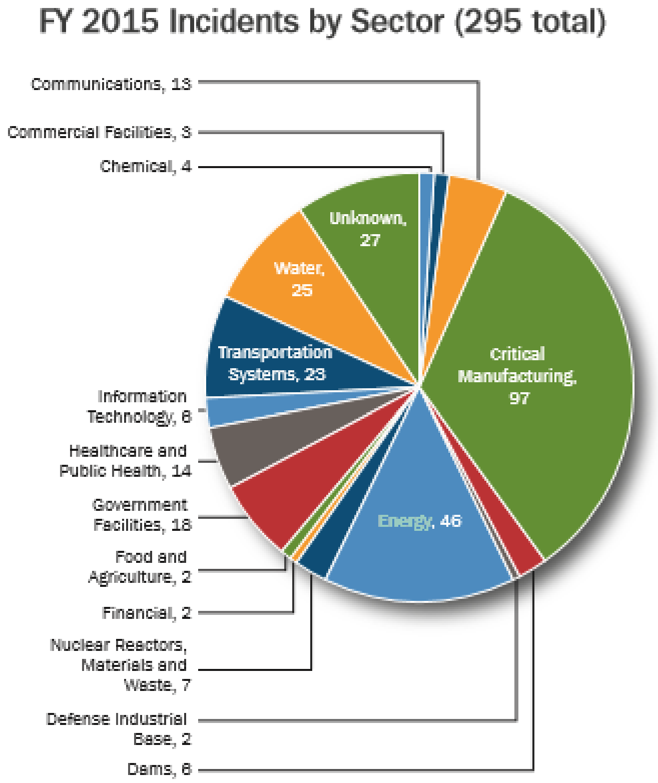


Figure 3-5 Incident Response FY 2015 Metrics

(Source - NCCIC/ICS-CERT, 2015)

- Bajpai et al, cautions that there is a great possibility for cyber-attacks to any cyber based which can destroy the Oil & Gas infrastructure without even gaining physically accessing the facilities. (Bajpai, S., & Gupta, J. P, 2007).
- Booz Allen Hamilton recommends that Oil & Gas companies must deploy end-to-end approach across their ecosystems—from upstream to downstream, business to operations—to thrive in the face of today's cyber challenge. (Booz Allen Hamilton, 2015).
- According to the 2016 study of Ponemon Institute sponsored by HP, costs of cybercrime for 17 different industry sectors have been compared, the cost of cybercrime for companies in Utilities & Energy experienced the 2nd highest annualized costs of app US$ 15million. (Ponemon Institute, 2016)

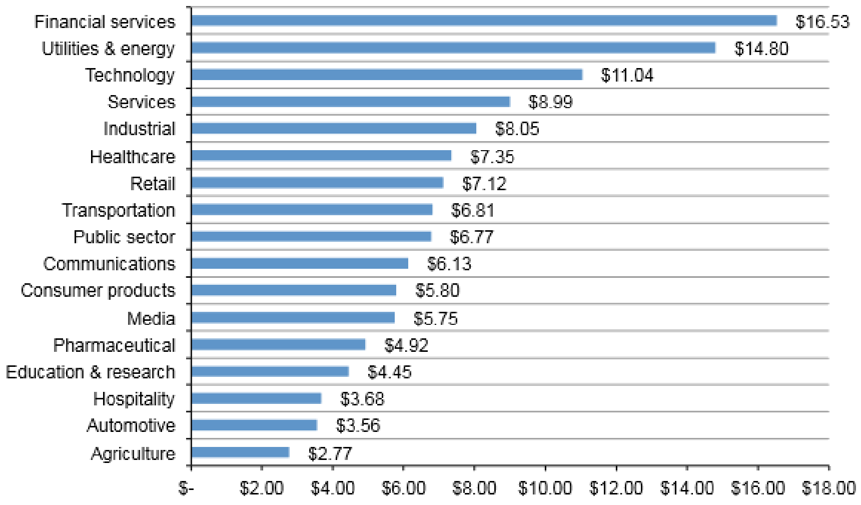


Figure 3-6 The Cost of Cyber Crime Impacts All Industries

(Source – Ponemon Institute, 2016)

- The National Critical Infrastructure are under threat has been established in the numerous literature that were reviewed, what stands out is that while the threat is prevalent across all the sectors, over the half the attacks are focused on the energy sector (Nicholson Webber et al., 2012). This assessment is shared and corroborated by other researchers as well, who have come to similar conclusions. This pattern of targeted cyber-attacks focused on the energy sector has remained a consistent phenomenon in the recent years. The analysis of the data show that not only have the percentage of attacks targeting the energy sector increased; there has also been an increase in the volume of attacks on the energy sector. (Nicholson Webber et al., 2012)

3.5.4 CYBER THREATS IN INDIA

- Under the aegis of the National Technical & Research Organization (NTRO), the National Crucial information Infrastructure Protection Centre (NCIIPC) was formed. (NCIIPC, 2014). This centre was created to come up with a remedy along with private corporate & other security organization which operate the critical sectors. They had a notification, which defined the critical sector as sectors that are critical to the nation and whose breakdown or destruction will have devastating damage on security of the nation, economy, civic health or safety. (NCIIPC, 2014). The government has categorized 12 sectors that meet the above requirement and hence covered them under the NCIIPC project as per the Section 70A of the amended IT Act. The sectors covered are from energy to power, manufacturing, aviation, defense, space, law enforcement and banking. (NCIIPC, 2014).

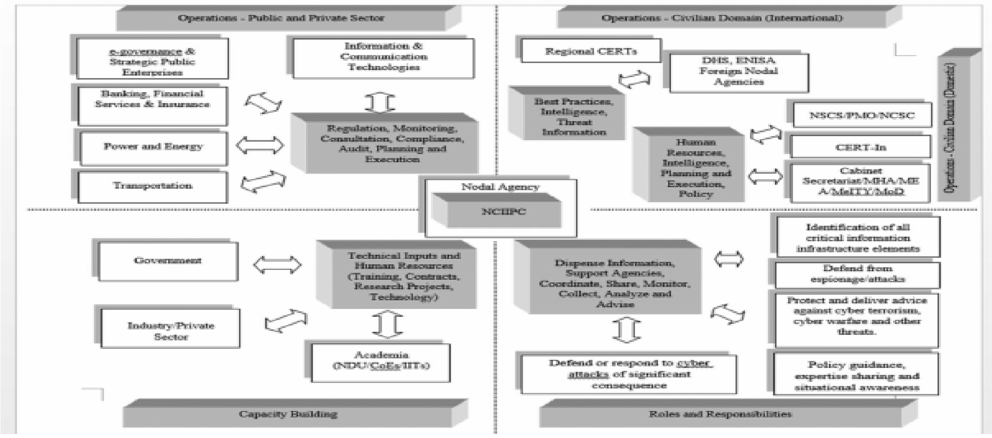

Operations - Public and Private Sector
e-governance & Strategic Public Enterprises
Information & Communication Technologies
Banking, Financial Services & Insurance
Regulation, Monitoring, Consultation, Compliance, Audit, Planning and Execution
Power and Energy
Transportation
Nodal Agency
NCIIPC
Government
Technical Inputs and Human Resources (Training, Contracts, Research Projects, Technology)
Industry/Private Sector
Academia (NDU/CoEs/IITs)
Capacity Building
Operations - Civilian Domain (International)
Regional CERTs
DHS, ENISA Foreign Nodal Agencies
Best Practices, Intelligence, Threat Information
NSCS/PMO/NCSC
Human Resources, Intelligence, Planning and Execution, Policy
CERT-In
Cabinet Secretariat/MHA/MEA/MeITY/MoD
Operations - Civilian Domain (Domestic)
Identification of all critical information infrastructure elements
Dispense Information, Support Agencies, Coordinate, Share, Monitor, Collect, Analyze and Advise
Defend from espionage/attacks
Protect and deliver advice against cyber terrorism, cyber warfare and other threats.
Defend or respond to cyber attacks of significant consequence
Policy guidance, expertise sharing and situational awareness
Roles and Responsibilities

Figure 3-7 CIIP in India: Possible Interactions among the Stakeholders (Source – NCIIPC)

- Protection of Crucial information Infrastructure (CII) is of supreme concern to governments worldwide. The Indian Government has notified the ‘National Critical

Information Infrastructure Protection Centre' as the pivotal agency vide Gazette of India notification on 16th January 2014, to address this threat. (NCIIPC, 2014).

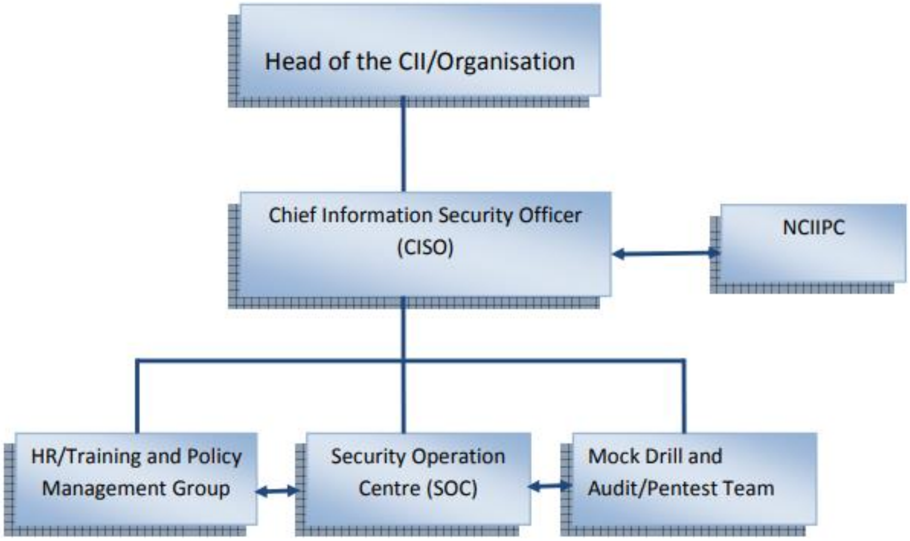

Head of the CII/Organisation
Chief Information Security Officer (CISO)
NCIIPC
HR/Training and Policy Management Group
Security Operation Centre (SOC)
Mock Drill and Audit/Pentest Team

Figure 3-8 Typical Structure of an Information Infrastructure

(Source – NCIIPC)

- Datta Saikat says that there has been a delay in the development of sector-specific guidelines and SoPs, leaving major vulnerabilities unaddressed. (Saikat Datta, 2016). He briefly outlines the history of NCIIPC formation and also scrutinize the major challenges or limitations of NCIIPC which are as follows:-
  - The structure of NCIIPC and the canards in the NCIIPC framework, used for ranking the sectors in order of criticality
  - The lack of domain-specific guidelines and Standard Operating Procedures (SoPs).

  Datta highlights how each of these limitations contributes towards the vulnerabilities in the India's Critical Information Infrastructure (CII). (Saikat Datta, 2016)

- Gupta.M. et al. propose that the present ICT infrastructure as well the proposed ICT Infrastructures of the country, whether they are in public or private domain should be examined by the experts from the National Disaster Management Authority (NDMA) so as to recommend appropriate working measures to reduce their vulnerability. (Gupta.M. et al, 2009). This would involve thorough technical investigation of the ICT systems. (Gupta.M. et al, 2009) This initiative may help in removing the redundant efforts. Disasters cannot be fully taken under control just by the capabilities of technology. The most vital aspect in any such initiative is the involvement from all stakeholders concerned. (Gupta.M. et al, 2009).

- Chaturvedi, M. et al. expresses concern that the cybersecurity effort in Indian context looks like patchy and cryptic. (Gupta, M., Bhattacharya, J., & Chaturvedi, M. M, 2009). They add that cybersecurity measures taken by relevant bodies and agencies are not available in public domain and therefore, seem to lack a probable lapse. (Gupta, M., Bhattacharya, J., & Chaturvedi, M. M, 2009).
- The taskforce Report of the Institute of Defense Strategy and Analysis (IDSA) on "India's Cybersecurity Challenges" suggests that both Government and the private sector shall jointly work together while executing their security and risk management plans. (IDSA, 2012) The purpose of the report is also to arouse public discussion, specifically among the security groups, in an extensive manner. (IDSA, 2012).
- Sameer Patil says that most of the SCADA systems are legacy systems and quite old, may be before the advent of the internet technology. These old systems, were never integrated to other systems. Since they were not designed to meet today's network, they always have potential cyber threats. (Sameer Patil, 2014) As per the industry circle, even many of the latest SCADA systems are prone for cyber-attacks, when integrated in a network. The reason is that many of the components behind the SCADA systems have narrow computational capability so as to run the security protocols. (Sameer Patil, 2014).
- Deepak Agarwal, Executive Director- IT, IOCL in an interview to Express Computer foresees three trends in India. (Express Computer, 2017) The first one is to see a comprehensive security solution. The second trend is a massive surge in the IT budgets which accommodate a huge portion towards cybersecurity pieces.

Among the budget, anywhere between 15-20% would be reserved for cybersecurity as more and more customer services will be digitized. (Express Computer, 2017).

- In 2015, Oil and Natural Gas Corporation Limited (ONGC) had a great setback when the company lost Rs.197 crore, where cyber criminals slightly modified the company's e-mail address and made Saudi Aramco to electronically transfer payments to their account. (The Indian Express, 2015).
- In 2014, a Turkish hacking group hacked the website of Indian Oil Corporation Limited (IOCL). (The Economic Times, 2014).
- In 2015, police have registered cases against two former employees of the oil refinery project of Essar Group in Gujarat for intruding the company's computer network and sending sensitive data outside. (DataBreaches.net, 2015) It was found that two employees were doing this during their 'notice-period' after resigning. This theft caused huge financial loss as well damage the company's reputation. (DataBreaches.net, 2015).
- In 2013, on the advice of CERT, the ministry of Petroleum and Natural alerted the heads of oil marketing companies about the likelihood of cyber-attacks. (The Hindu, 2013).
- In 2017, Statoil decided to relocate its vital IT centre from its service provider HCL Technologies back to Norway to enhance cybersecurity. (Reuters, 2017). This was because of the occurance of many cybersecurity incidents in 2014, which also included an interruption in the oil terminal operations at the Mongstad refinery. This made Statoil to form a task force to do a risk assessment. Finally Statoil made a decision to do away with the service provider HCL. (Reuters, 2017) .
- Udbhav Tiwari in his report on the Indian Computer Emergency Response Team's role in the Indian Cybersecurity Ecosystem analyses the proactive, reactive and the training mandates of CERT-In respectively. The report also highlighted key areas that can be improved and suggesting normative measures using which such improvements can be carried out. the paper demonstrates with its analysis, CERT-In's mandate to proactively defend India's cybersecurity interest for the various stakeholders in the Indian Cybersecurity ecosystem could benefit from a number of

reforms. (Tiwari, U, (2016). Studying the best practices from various similar organizations across the world, especially the European Union and the USA along with a focused increase on original research & development and targeted public outreach are the three main ways to bring the CERT-in up to par to not only its peers from all over the world but also capable of pre-empting the increasingly complex threats in cybersecurity. (Tiwari, U, (2016).

- Parliament informed that more than 53,000 cybersecurity incidents were witnessed in the country in 2017. (Economic Times, 2018). IT Minister Mr. Ravi Shankar Prasad said in Rajya Sabha that the Indian Computer Emergency Response Team (CERT- In) had so far observed an average of 50,000 incidents between 2014 -17. (Economic Times, 2018).
- Rajabahadur V. Arcot, an automation consultant expresses concern about India's cyber threats. He feels that India has become more vulnerable, because of its geo-political pressures. (Rajabahadur V. Arcot, 2014) Though the government has approved NCIIPC to take care of the Critical Information Infrastructures across the country, there is very less information available in the public domain. Also the government has formed Indian Computer Emergency Response Team (CERT-In). But as on date, no reliable information about these initiatives is available, which creates a big anxiety. (Rajabahadur V. Arcot, 2014) The formation of NCIIPC demands raising cybersecurity awareness among all people concerned. But it is not doing justice for its duty by maintaining a low profile. In fact, the website of CERT-In itself is not available most of the time. (Rajabahadur V. Arcot, 2014).
- In 2016, the website of Hindustan Petroleum Corporation Limited (HPCL) was taken over by hackers. (CYWARE, 2017). The content of the website was tampered with a nasty link that could harm the system of anybody who visits the website. (CYWARE, 2017).
- Ananda Kumar et al. suggest a national policy guideline and a regulatory framework in the power sector across the value chain to address the cybersecurity issues. (Ananda Kumar et al, 2015).

3.5.5 Cost of Cyber Threats

- Ponemon Institute in their 2016 report on “Cost of Cyber Crime Study & the Risk of Business Innovation” mentions that the average cost of cyber-crime per annum differs sector to sector. The study in 2016, took 17 different industry sectors and visualized and compared the cost averages. From the survey, it was concluded that the highest annualized cost spent on cyber-crime are in the financial services and in the utilities & energy sectors. (Ponemon Institute, 2016).

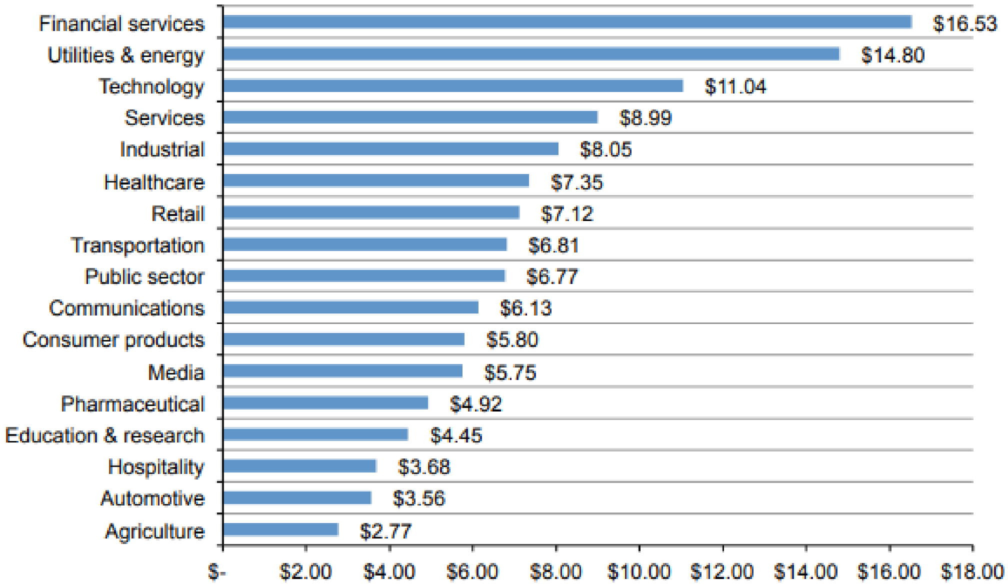


Figure 3-9 Average Annualized Cost by Industry Sector

(Source - Ponemon Institute, 2016)

3.5.6 Vulnerabilities Due To IT-OT Integration

- Thomas Garvin discusses that cybersecurity is an especially important collaboration area regarding IT/OT convergence. (Garvin, T, 2015). With the increasing amount of available data in the Internet of Everything and the number of sensor connections multiplying the possible failure or intrusion points. Process safety and cybersecurity should be considered together with the same level of concern. (Garvin, T, 2015).

- Baudoin, C. R. propose a roadmap for Industrial Internet application in O&G, give advice on organizing and governing such efforts and indicate resources that can help jumpstart such an effort. (Baudoin, C. R, 2016).
- Anshu Mittal et al, suggest that organizations should watchfully overseer IoT implementations during the early stage of the projects. (Anshu Mittal, Andrew Slaughter, & Paul Zonneveld, 2017). The authors have also mentioned that each business processes of the Oil & Gas value chain have distinct cyber vulnerability and severity profile.

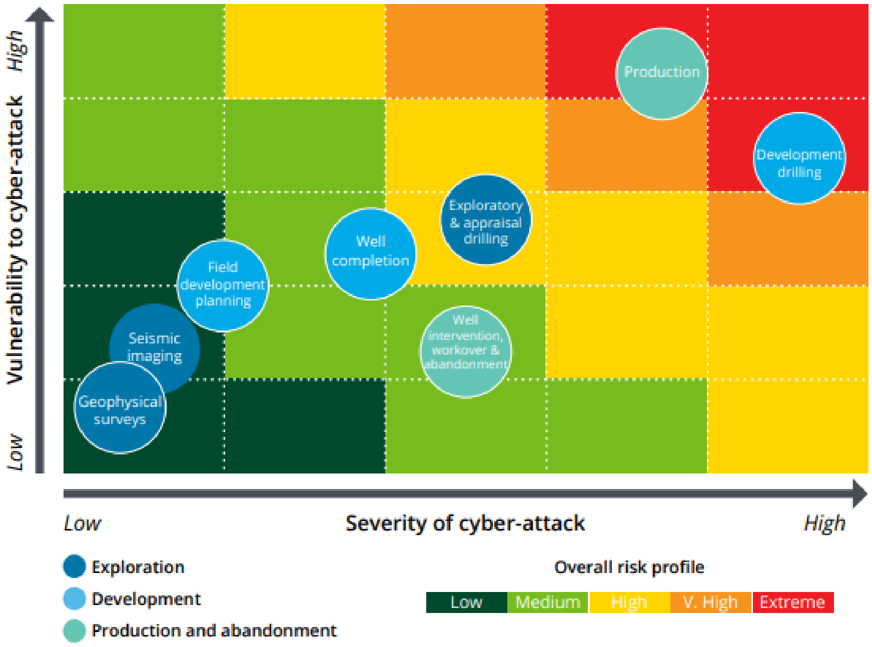


Figure 3-10 Cyber Vulnerability Matrix by Upstream Operations

(Source – Anshu Mittal et al at deloitte.com, 2017)

Mittal ET all have also highlighted that the industry's march toward interconnectedness has outpaced its cyber maturity, making it a prime target for cyber-attacks. (Anshu Mittal, Andrew Slaughter, & Paul Zonneveld, 2017). They believe that limited strategic appreciation and sponsorship at a boardroom level—

rather than lack of technical know-how—explain the industry's relatively low cyber maturity. Getting sponsorship from top management requires to explain the problem strategically and describing how cybersecurity enables the company's three topmost operational imperatives: safety of assets, people, and environment; an uninterrupted availability and reliability of assets; and creating new value from assets. (Anshu Mittal, Andrew Slaughter, & Paul Zonneveld, 2017).

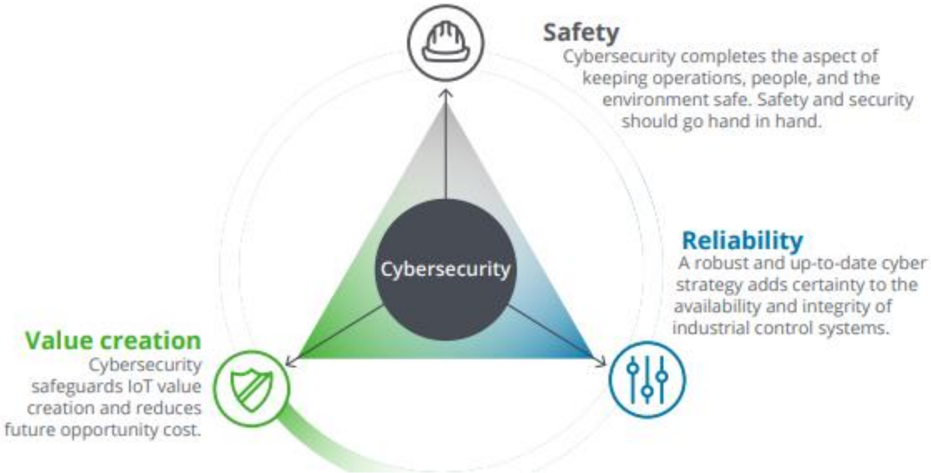

Safety
Cybersecurity completes the aspect of keeping operations, people, and the environment safe. Safety and security should go hand in hand.
Cybersecurity
Reliability
A robust and up-to-date cyber strategy adds certainty to the availability and integrity of industrial control systems.
Value creation
Cybersecurity safeguards IoT value creation and reduces future opportunity cost.

Figure 3-11 Cybersecurity Enables Safety, Reliability and Value

(Source – Anshu Mittal et al at deloitte.com, 2017)

- Ernst & Young (EY) in their Global Information Security Survey 2015 says that cybersecurity would be vital to unravelling innovation and growth. By adopting a risk-oriented style to cybersecurity, organizations can progress on new openings. (Ernst & Young, E&Y, 2015).
- The Ponemon Institute surveyed 377 stakeholders in the US who are responsible for cybersecurity in the upstream, midstream and downstream applications. (Ponemon Institute, 2017). Majority of them termed that their companies are in the premature stage of maturity in terms of their cyber readiness. (Ponemon Institute, 2017). The survey findings also revealed the following facts. 59 % thought that there is a larger threat in the OT landscape compared to the IT landscape. 61 % alleged that they are struggling in alleviating cyber risks through the Oil & Gas

value chain. (Ponemon Institute, 2017). 41 % said they consistently monitor OT landscape to take care of the vulnerabilities. 65 % thought that the critical cybersecurity threat is not given due importance in the organizations and 15 % of respondents said that the culprits may be from the organization itself. 61 % said that their plant automations are not adequately protected. (Ponemon Institute, 2017).

- Ciepiela says that in the past, Operational Technology (OT) networks were distanced from the internet, but today, they have to be interconnected. (Ciepiela, P, 2017). A cyberattack on an OT infrastructure may have serious problems that may include outages of services, damage to environmental and even fatality. (Ciepiela, P, 2017).

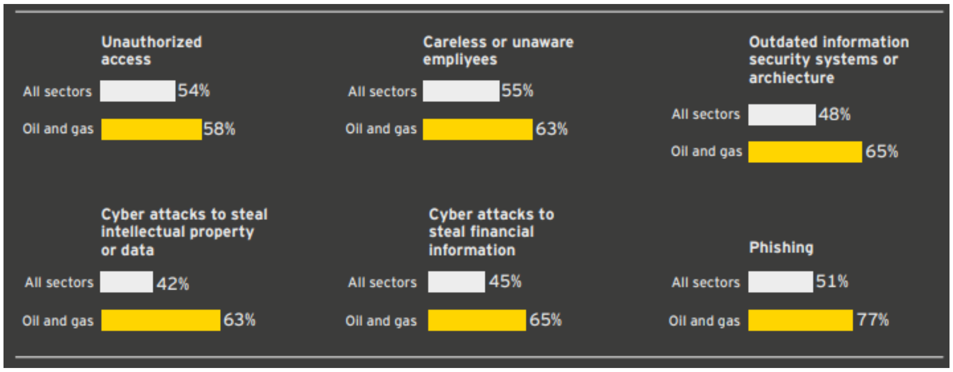


Figure 3-12 Comparison of Cyber Threats Across Industry

(Source - Ernst & Young, E&Y, 2017)

The technological stride in the petroleum industry increases since the industry organizes itself for a substantial transformation. Global Information Security Survey by EY in 2016-17 demonstrates that Oil & Gas companies are moving in a direction to sense and fight the cyberattacks and threats. But at the same time, the results show the necessity for better resilience. (Ernst & Young, E&Y, 2017).

- Joel Parshal says that cyber defense is much more than a digital or IT issue. It carries implications for every dimension of business, including health, safety, environmental, and financial activity. (Joel Parshall, 2018). Cybersecurity experts are adamant that operations technology (OT) systems cannot be viewed as safe simply because they are not IT systems. While they have differing characteristics, IT and OT systems must be viewed as a continuum. (Joel Parshall, 2018).

- Business Advantage conducted a research study of ICS/OT cybersecurity professionals to understand their attitudes and to detect the most crucial cybersecurity issues distressing the companies. Industrial cybersecurity incidents happened repeatedly. (Business Advantage, 2017). But in spite of alertness and preparedness for infringements, companies often miscalculate both the origin and effects of such cyber incidents. (Business Advantage, 2017). It’s crucial that efforts are taken to detect the ICS related risks. By placing thorough strategies and measures in place to manage risks, companies put themselves in the best possible position to secure their operational technology. (Business Advantage, 2017).

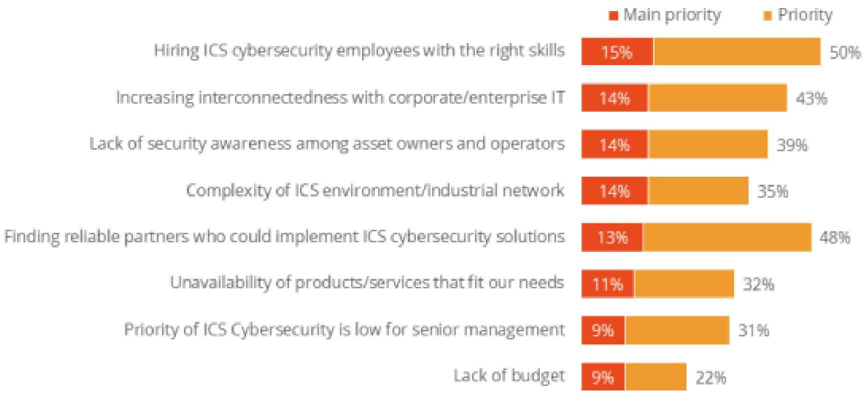


Figure 3-13 Challenges of Managing ICS Cybersecurity

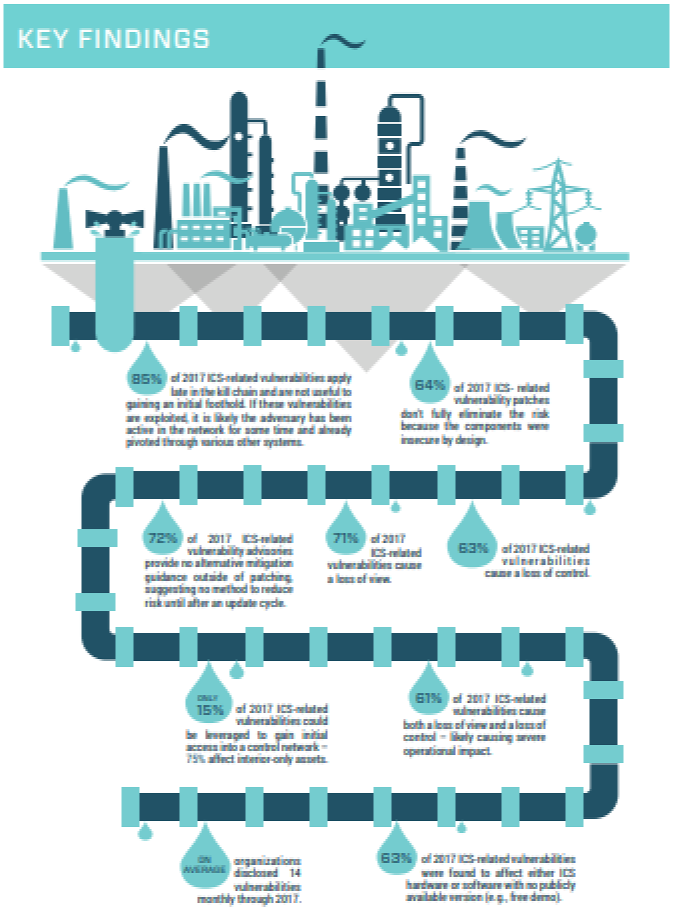
(Source - Business Advantage, 2017)

The report summary gives an outline of the cybersecurity issues or cyber risks facing the organizations. This is in particular to organization that run ICS environments. (Business Advantage, 2017).

- From the CISO Platform Annual Summit, Amit observes that the panel has concluded e of the Top Threats & Controls for IoT Security as following:
  Risks and security imperatives in Industrial IoT (CISO Platform, 2017).

1. Operational Technology (OT) control systems which are more connected to the internet and outside world, which has more exposure has major risk and also it is not designed to protect against these attacks. (CISO Platform, 2017).
2. Physical security on the periphery of industrial assets alone does not reduce the risks any longer and the industry that uses OT control systems should have layered cyber controls. (CISO Platform, 2017).
3. Securing OT is about protecting control over the cyber physical threats. The goal is to protect people, production, and assets. (CISO Platform, 2017).
4. When we compare IT vs OT, we find, IT in all companies have been connected to wild world of internet and our enterprise security controls have matured over time. However, same is not true for Operational technology (OT) that runs factories and plants. OT has not gone through learning cycles like IT. In factories, you will find lot of aged infrastructure systems that were not meant to be connected to the outside world. This poses a serious threat. (CISO Platform, 2017).
5. OT is all about very Safe, very Efficient, Productive systems & processes with long lived missions. So when compared with IT, the downtimes or regular patching are rare. Exposures here can stay for a very long time. (CISO Platform, 2017).
6. In OT world, while attack vectors might be same but consequences are different, so industrial cybersecurity needs very specialized approach to protect it. (CISO Platform, 2017).

- Dragos identified that 2017 denotes a significant year in the security of Industrial Control System (ICS). This year saw two key and excpetional ICS-disruptive attackers of ICS; Also identified five divergent activity groups that were pursuing networks of ICS. There were many massive events of IT infection occurred that had sever implications in the ICS system. (Dragos, 2017). Dragos tracked 163 vulnerability issues with an industrial control system (ICS) in 2017. Among these, most of them were vulnerabilities in poorly secured products within the ICS network. (Dragos, 2017).



85% of 2017 ICS-related vulnerabilities apply late in the kill chain and are not useful to gaining an initial foothold. If these vulnerabilities are exploited, it is likely the adversary has been active in the network for some time and already pivoted through various other systems.

64% of 2017 ICS- related vulnerability patches don't fully eliminate the risk because the components were insecure by design.

72% of 2017 ICS-related vulnerability advisories provide no alternative mitigation guidance outside of patching, suggesting no method to reduce risk until after an update cycle.

71% of 2017 ICS-related vulnerabilities cause a loss of view.

63% of 2017 ICS-related vulnerabilities cause a loss of control.

ONLY 15% of 2017 ICS-related vulnerabilities could be leveraged to gain initial access into a control network – 75% affect interior-only assets.

61% of 2017 ICS-related vulnerabilities cause both a loss of view and a loss of control – likely causing severe operational impact.

ON AVERAGE organizations disclosed 14 vulnerabilities monthly through 2017.

63% of 2017 ICS-related vulnerabilities were found to affect either ICS hardware or software with no publicly available version (e.g., free demo).

Figure 3-14 Key Findings of 2017 ICS-Related Vulnerabilities

(Source - Dragos, 2017)

- Dragos discovered that public reports were typically unsuccessful to sufficiently outline the industrial effects of vulnerabilities. Many of the public vulnerability disclosure reports provide no alternative guidance beyond, patch, or use secure networks, Dragos could see massive scope for progress in the disclosure reports system. (Dragos, 2017).
- Farooq Shaik et al. mentions that protecting digital infrastructures and assets against cyber-attacks will be critical for survival. (Farooq Shaik, Arif Abdullah, S. K, 2017). They add that being a leading industry in the world, Oil & Gas companies that expand their business into the digital network will have to proactively look

beyond individual security measures. Security needs to be addressed holistically, along the business processes of their organization – internal as well as those related to their customers and vendors, covering the entire supply chain. First and foremost, this implies focusing on the corporate security strategy. (Farooq Shaik, Arif Abdullah, S. K, 2017).

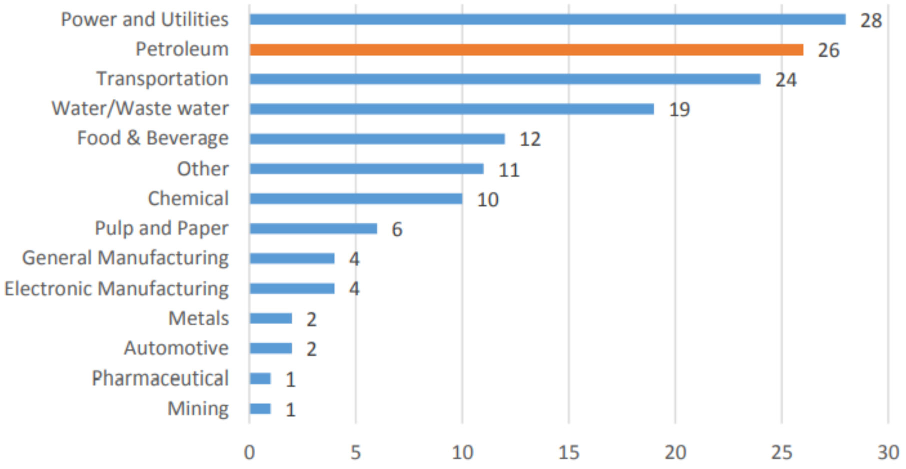


Figure 3-15 Relative Attack Frequency on Different Industries

(Source: Repository of Industrial Security Incidents/Security Incidents Org)

Organizations in Oil & Gas industry face huge threats, such as Interruption of Utilities, Hydrocarbon Installation Terrorism, Plant Sabotage, IT Infrastructure disruption, plant shutdown and even Data/Device Corruption. With the Oil & Gas industry being part of our everyday life protecting their critical infrastructure has never been more crucial. (Farooq Shaik, Arif Abdullah, S. K, 2017).

- Marc Goodman crisply summarizes the challenge of our times, “When everything is connected, everybody is vulnerable” (Goodman, 2015). As technology advances and progresses towards a smarter world – a world of smart devices, smart meters, smart cities and they get inter-connected into a mesh of Internet Protocol (IP) enabled infrastructure that interact with each other to improve productivity, lifestyle and how we interact with each other, it also exposes us to risks.
- Industrial Control Systems (ICS) are the systems which monitor and control various paramets such as Pressure, Temperature, Flow etc in a complicated proceses in the

industry. It could be in the areas of Refining, Chemicals manufacturing, or Electic power generation and transmission. Today the latest ICS infrastructures typically comprise of various types of smart, microprocessor based system, interconnecting over complicatyed and distributed network system. (Systems and Network Analysis Center, National Security Agency, 2010).

- The last few years has seen an exponential increase in control system vulnerabilities, Knapp and Langill point out that 85% of the known control system in the Open-Source Vulnerabilities Database (OSVDB) was just over the last three years from 2011 to 2014 (Knapp & Langill, 2015).

3.5.7 CYBERSECURITY REGULATIONS IN THE OIL & GAS INDUSTRY

3.5.7.1 Regulatory Interventions in the USA

In the USA, the Electricity Subsector and the Oil & Natural Gas Subsector each have customized standards towards cybersecurity. This is used by many organizations either willingly or by requirement, in addition to the cross-sector Informative References identified in the Framework Core. It is also found that few, like C2M2 model are generally applicable or have tailored versions for each and every subsectors. (Department of Energy, USA, 2014).

Looking into the Cybersecurity Capability Maturity Model (C2M2), it was developed by various Government agencies and the Department of Energy (DOE) and contributors from industry. It is developed to help critical infrastructure organizations to evaluate and possibly improve their cybersecurity practices. If any energy sector organization wants to implement the Cybersecurity Framework (NIST 2014), they can use this model. The C2M2 includes a self-evaluation toolkit that guides each organization to identify its cybersecurity and risk management practices, map them to specific levels of maturity within the model, set target maturity levels, and identify gaps and potential practices that allow the organization to mature over time. The C2M2 covers all of the practices of the Framework The

C2M2 and its supporting guide for the toolkit helps an organization to identify its Current Profile and to establish a Target Profile. (department, USA, 2014).

With the help of the C2M2 toolkit, every organizations can do a self-assessment of their current processes. Each section is separated into a set of goals which can be functional to them as well. (Department of Energy, USA, 2014).

- The Oil and Natural Gas Information Sharing Analysis Center (ONG-ISAC) provides a safe and trustworthy system for exchanging cybersecurity related information between the oil and natural gas industry in the USA. (ONG-ISAC, 2016) It provides relevant cybersecurity information to integrated oil, natural gas, upstream, mid-stream and down-stream companies, field services, including industry associations and energy service and supply companies. (ONG-ISAC, 2016).
- The Downstream Natural Gas Information Sharing Analysis Center (DNG-ISAC) serves the natural gas utility distribution companies in the USA, by enabling communications between various stakeholders. (DNG-ISAC, 2016).
- The Interstate Natural Gas Association of America (INGAA) standards help the natural gas pipelines companies to cope with cybersecurity needs of the control systems. (INGAA, 2009). The Cyber and Physical Security Committee works to ensure the physical and cybersecurity of natural gas pipeline systems. (INGAA, 2009). On a federal regulatory level, the committee primarily works with the Department of Homeland Security (DHS), the Transportation Safety Administration, the Federal Energy Regulatory Commission (FERC), the Department of Energy (DOE), other agencies and Congress on matters of related to take care of the safety and reliability of the nation’s pipeline network. This group shares with the government and holds security exercises and participates in information sharing to carefully alert in cyber and physical threats. (INGAA, 2009).
- ANSI/API STD 780 is the standard for the Security Risk Assessment (SRA) Methodology for the Petroleum and Petrochemical Industries. (Moore, D. A., 2013) This Standard’s role is to facilitate the petroleum & petrochemical industries in

knowing to conduct SRAs. (Moore, D. A., 2013). Since all Industries faces all types of security issues, this standard defines the suggested approach for assessing security risk. (Moore, D. A., 2013).The standard is meant for those accountable in condu cting SRAs and managing security at these facilities. (Moore, D. A., 2013).The API SRA procedure is applicable for the petroleum sector, for a broad range of fixed as well as mobile applications. (Moore, D. A., 2013).

- Chemical Facility Anti-Terrorism Standards (CFATS) is the prime regulatory initiative focused precisely on security at risk oriented hazardous chemical facilities. (DHS, 2018). This CFATS program is controlled by the Department of Homeland Security (DHS), with the help of the Infrastructure Security Compliance Division (ISCD). (DHS, 2018). For companies dealing with chemicals, the guidance on physical as well cybersecurity is offered by the Risk Based Performance Standards (RBPS) of the Department of Homeland Security. (DHS, 2018).
- In 2014, the National Institute of Standards and Technology (NIST) issued the voluntary guideline for enhancing Critical Infrastructure Cybersecurity, so that organizations can use the same to evaluate and manage cybersecurity risk. (NIST, 2014).
- In order to develop cybersecurity standards, tools, and processes, Energy sectors have a good background and reputation of working together to guarantee nonstop service. The Department of Energy (DOE) in US, as an agency developed cybersecurity framework execution guidance and worked with Coordinating Councils of the Electricity Subsector as well the Oil & Natural Gas Subsector and others. (Department of Energy, 2015). This was mainly for energy sector owners and operators, which will help the organizations to execute the framework to reduce cyber-attacks. (Department of Energy, 2015).
- In 2004, US Department of Homeland Security (DHS) has come out with a report on “A Comparison of Oil & Gas Segment Cybersecurity Standards”. A comparative study is done on the security standards developed for the Oil & Gas critical infrastructures. (US Department of Homeland Security, 2004). Though there are

many standards that take care of control system cybersecurity, all of them use ISO/IEC 17799 as the base standard. (US Department of Homeland Security, 2004).

3.5.7.2 Regulatory Interventions in the Europe

According to a 2015 survey, nearly 80% of European companies have faced at least one cybersecurity incident in one year and the number of security incidents across all industries increased by 38%. (European Commission, 2016). More specifically, the energy sector is highly dependent on secure network and information systems. It is seen that cyber-attacks are more in Major gas and electricity companies by commercial and criminal intent. Symantec noted that an average of 74 attacks per day were launched in the world between 2012 and 2013 and that 16% of these attacks targeted the energy sector (Symantec, 2014), illustrating the need for an efficient sharing of cybersecurity information in the energy sector. The recent cyber-attacks against power plants in Ukraine (ICS-CERT, 2016) shown that information sharing is “key in the identification of a coordinated attack and directing appropriate response actions” (E-ISAC and SANS, 2016).

- The National Cybersecurity Centre (NCSC) Energy ISAC is a Dutch public-private partnership, which enables participants to exchange information and experiences about cybersecurity in the energy sector. This ISAC also enables participants to build up trust among each other and informally exchange knowledge and experience on cybersecurity related issues. (NSSC, n.d.).
- The Cybersecurity Information Sharing Partnership (CiSP) is a UK’s collaborative initiative between industry and government that enables its members to exchange information related to cyber threats, while protecting the confidentiality of the shared information. (ncsc.gov.uk, 2016).
- Statoil CSIRT, in Norway, provides cybersecurity incident response capabilities to Statoil (Oil & Gas) and to its joint ventures. The Statoil CSIRT is currently involved in information sharing initiatives with other government and private entities in

Norway and the UK on specific cyber threats affecting the Oil & Gas subsector. (FIRST, n.d.).

- In addition, Austria is in the process of implementing a CSIRT for the energy sector that will be responsible for the reception and sharing of cybersecurity related information and other vulnerabilities in the sector (CyberWiser, n.d). The CSIRT will support Austrian energy companies in their response to cybersecurity incidents and will collaborate with public organizations such as the NRAs, critical infrastructure providers and public authorities. (CyberWiser, n.d)..
- The European Commission set up an Energy Expert Cybersecurity Platform (EECSP) which is an informal and temporary commission of expert group on cybersecurity. (ENCS, n.d.) The tasks of the special group is to provide direction to the European Commission on policy and regulatory directions by addressing the infrastructural issues as well the security system in the sector. (ENCS, n.d.).
- Thematic Network on Critical Energy Infrastructure Protection (TNCEIP) is a scheme of the DG Energy of the European Commission. It comprises of the owners and operators of energy infrastructure which include sectors of electricity, gas and oil in Europe. It permits the operators in energy sector to swap cyber security related information. (European Commission, 2012).
- The Incident and Threat Information Sharing EU Centre (ITIS-EUC) aims to enhance the cyber security awareness of critical energy infrastructures by providing information on incidents and emerging threats and fostering information sharing among the relevant energy stakeholders. ITIS is an initiative of DG Energy and its operation (portal maintenance, content, user support) is entrusted to DG JRC [Joint Research Centre] of the European Commission (European Commission, n.d.)..
- The Dutch National Cybersecurity Centre (NCSC) launched an information sharing initiative to support the energy sector in the identification of relevant cyber threats, vulnerabilities and cybersecurity good practice. (NSSC, n.d).
- In 2013, France passed a military programming law that gives ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information, the National Cybersecurity Agency of France) the ability to set minimum cybersecurity requirements at the

technical and organizational levels for operators of critical infrastructures. In order to define rules that are efficient, compatible with the specific context of each sector, and economically viable, ANSSI created and steers sectorial working groups. Each of these groups gathers, for a given sector, the critical infrastructures operators, the coordinating ministries and the sectoral authorities. (ANSSI, n.d.).

- In 2005, the UK Centre for the Protection of the National Infrastructures (CPNI) set up the European SCADA and Control Systems Information Exchange (EUROSCSIE). The initiative was created to address the increasing number of cyber threats and the potential effects of cyber-attacks against industrial control systems. (GCSC, n.d.) The initiative is composed of members of the EU governments, research institutions, operators and industries that depend or are responsible for the security of critical infrastructure' industrial control systems. ENISA runs the secretariat for this expert group now. (GCSC, n.d.).
- The European Energy Information Sharing Analysis Centre (EE-ISAC) is a main outcome of the Distributed Energy Security Knowledge (DENSEK) project19. EE-ISAC was established in 2015. Its creation responds to the need for European collaboration in protecting the energy sector from cyber-attacks. (EE-ISAC, n.d.) EE-ISAC is a network of trust in which private and public parties share security information via member meetings, via an information sharing platform or via situational awareness networks. (EE-ISAC, n.d.).
- The National Cybersecurity Centre (NCSC) Energy ISAC is a Dutch public-private partnership, which enables participants to exchange information and experiences about cybersecurity in the energy sector. (ncsc.nl) This ISAC also enables participants to build up trust among each other and informally exchange knowledge and experience on cybersecurity issues.
- Kraft CERT (Norwegian energy sector CERT) provides support for the entire power industry in preventing and handling security incidents. (KraftCERT, n.d.) The CERT is specialized in monitoring, counselling and incident response and facilitates exchange of security incidents information between its members. (KraftCERT, n.d.).

- SI-CERT (Slovenian Computer Emergency Response Team) is the national cyber security incident response center. (SI-CERT. (n.d.) It coordinates incident resolution, technical consulting on intrusions, computer infections and other abuses and issues warnings on current threats in electronic networks for network operators and the general public. (SI-CERT. (n.d.) SI-CERT independently operates the Safe on the internet national awareness program and participates in the SAFE-SI project. SI-CERT operates within the framework of the Arnes (Academic and Research Network of Slovenia) public institute. (SI-CERT. (n.d.).
- The set-up of the Critical Infrastructure Warning Information Network (CIWIN) is one of the measures foreseen to enable the execution of the European Program for Critical Infrastructure Protection (EPCIP). (European Commission, (n.d.) The set-up intended to assist Member States and the European Commission facilitate exchange of cyber related information towards protection of Critical Infrastructure Protection (CIP). (European Commission, (n.d.).
- The European Commission set up an Energy Expert Cybersecurity Platform (EECSP) composed of a specialist group (European Commission, 2015a) (European Commission, (n.d.) The specialist group is an informal and temporary commission expert group on cybersecurity. (European Commission, (n.d.) The task of the specialist group is to deliver direction to the European Commission on vital security issues related to the infrastructures. (European Commission, (n.d.).
- Incident and Threat Information Sharing EU Centre is an Open Source Intelligence for the Energy Sector. . (European Commission, (n.d.) ITIS collects open source information on incidents and threats (all-hazards approach), performs analysis and distributes this to trusted partners in the energy sector. The ITIS office is physically located in JRC premises in Ispra, Italy. . (European Commission, (n.d.).
- The European Network for Cybersecurity (ENCS) established in 2012 brought together the stakeholders and security experts of critical infrastructure to position secure critical energy grids and infrastructure in Europe. (ENCS, n.d.)The ENCS provides cybersecurity solutions and counsel to grid operators and regulators. The research based services of ENCS include collaboration projects among member,

and testing aspects of the security. It further extends to training, information sharing and knowledge sharing. (ENCS, n.d.) The information and knowledge sharing service comprise of assembly meetings, security roundtables, member and partner events, webinars and a portal with content and good practices created by ENCS experts and correlated members and partners. (ENCS, n.d.).

- In 2005, the UK Centre for the Protection of the National Infrastructures (CPNI) set up the European SCADA and Control Systems Information Exchange (EUROSCSIE). (ENISA, n.d.) This setup was formed to tackle the growing number of cyber threats and the potential effects of cyber-attacks against industrial control systems. The initiative is composed of members of the EU governments, research institutions, operators and industries that depend or are responsible for the security of critical infrastructure' industrial control systems. ENISA runs the secretariat for this expert group now. (ENISA, n.d.).
- CERT.at is the Austrian national CERT. It is the chief contact point for IT related at a national level. The body will also will coordinate with other CERTs operating in that geography. (CERT.at, n.d.) They would provide the basic IT related security information such as warnings, alerts, advice etc. for the Subject Matter Experts (SMEs). (CERT.at, n.d.).
- Recognizing the surge in number and the complexity of cyberattacks, in 2008 France acknowledged that there is a need for strategic priority to strengthen the cybersecurity of CIIP. (ANSSI, n.d.). In 2013, a specific CIIP regulatory framework was established under the name CIIP law. France identified 12 sectors as critical which had more than 200 public and private operators and ensure that this law will be ordained in them. (ANSSI, n.d.).
- The Cyber Security Strategy for Germany was approved in 2011. (KRITIS, (n.d.). Its objective is to ensure cybersecurity so that it considers the significance and the desirability of protecting the networked information infrastructure without compromising the opportunities and benefits of cyber space. (kritis.bund.de, 2011) The Implementation Plan CIP (KRITIS) is Germany's substantial contribution to

the announced "European Program for Critical Infrastructure Protection" (EPCIP). (KRITIS, (n.d.).

- Aubuchon et al. describe the Linking Oil & Gas Industry to Improve Cybersecurity (LOGIIC) model and explains how the cyber challenged can be addresses when the industries collaborate with the government bodies, process control vendors and security technology vendors. (DHS, 2004).
- The Department of Energy (DOE), US has come out with an industry-specific **C**ybersecurity **C**apability **M**aturity **M**odel (ONG-C2M2) for the Oil and Natural Gas (ONG) industry, so that they can evaluate and execute their cybersecurity programs. (Department of Energy, USA, 2014).
- Kambour, A. says that through proper risk management and coordination with the private sector, governmental agencies, and neighboring states, governors can help guarantee that the private energy networks are adequately taken care from cyber threats while strengthening their ability to lead response and recovery planning. (Andrew Kambour, 2014).
- Jason Holcomb in his “Definitive Guide to Cybersecurity for the Oil & Gas Industry” says that in addition to the traditional physical and operational risks faced by the industry, the Oil and Gas industry also is vulnerable to the escalating risk of cyberattacks that also intimidate its stakeholders. (Jason Holcomb, 2016). He also adds that there is little regulation of cybersecurity in the Oil & Gas sector, but there is a body of standards and best practices from both industry and government to help companies ensure that their policies and status meet their needs for securing their own infrastructures and data. (Jason Holcomb, 2016) They also ensure that companies are capable to meet the needs of partners and customers. (Jason Holcomb, 2016). While these are guidelines—voluntary and not mandatory—a company that ignores cybersecurity policies and procedures that have become recognized as best practices in the industry could find itself not only at greater risk to cyber threats, but also a threat to the rest of the ecosystem in which it operates. (Jason Holcomb, 2016).

- Tim Lester in his report on “Cybersecurity: A growing threat to the energy sector An Australian perspective” says that a society's dependence on technology increases and there is a corresponding need for cybersecurity to be taken more seriously. (Tim Lester, 2016). A cyber-attack can target critical infrastructure or physical facilities, or disrupt an entire network's functionality. (Tim Lester, 2016). The repercussions of a cyber-attack in the energy sector can be especially extensive and thus, it would be prudent for businesses to be cyber resilient. (Tim Lester, 2016) For some, this may involve adopting regulatory frameworks or ensuring that compliance obligations are being met. (Tim Lester, 2016). Irrespective of a company's size, nature of business or location, it is important to be aware of the risks and to be protected against potentially irreversible and costly damage. (Tim Lester, 2016).

3.5.8 ROLE OF SENOR LEADERS IN CYBERSECURITY

- François, M. et al. argues that while monitoring, repelling, and responding to cyber-threats while meeting compliance requirements are well-established duties of Chief Information Security Officers (CISOs). They also need to take a stronger and more strategic leadership role in the coming days. (Taryn Aguas, Khalid Kark, & Monique François, 2016). CISOs tend to serve as “technologists” by managing key functions of security technologies as a “guardians” in safeguarding the enterprise assets. Going forward, they need to act as “strategists” by focusing more on security strategies and also act as “advisors” by advising CXO community the importance of security. (Taryn Aguas, Khalid Kark, & Monique François, 2016).

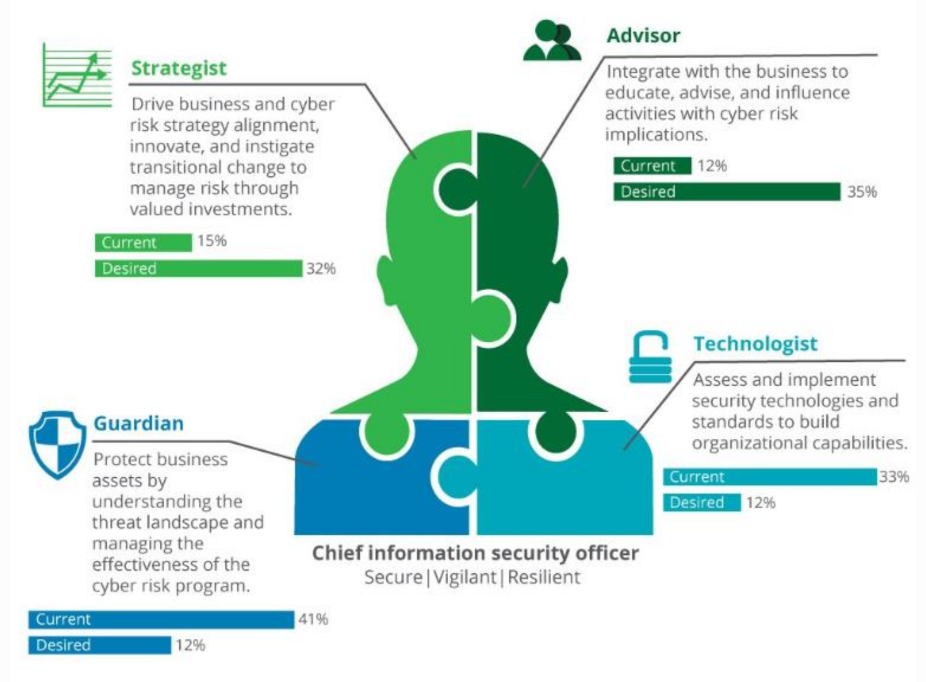


Figure 3-16 The Four Faces of the CISO

(Source - Jim Eckenrode, Sam Friedman at Deloitte, 2018)

- Morse S et al. highlights the role of CISO and their growing importance. The Chief Information Security Officer (CISO) role in the Oil & Gas is to carry out the cybersecurity agenda set by facilitating the senior management and the Board of Directors. In Oil & Gas, physical security is directly linked to cybersecurity, as cyberattacks could prove interruptive or even fatal to thousands if not millions of people. (Jennifer Rockwood, & Stephen C. Morse, 2015). This possible disaster is increasing the scope of skills needed to be an effective CISO. (Jennifer Rockwood, & Stephen C. Morse, 2015).
- Tripwire Guest Authors stresses that the senior management team has a greater accountability, more than just creating risk framework. They should ensure that they should be fully involved in all aspects of cyber risks and establish a perfect organized effort within the companies. (Reza, Tripwire, 2016).

- McKinsey in their article “Why senior leaders are the front line against cyberattacks” mentions though all companies are conscious of the growing risk, yet few are involving in length & breadth to protect all crucial information. (McKinsey & Company, 2014).
- Katharina Rick ET all says that companies have been deepening their attention on cybersecurity across the industries. This is primarily due to digitalization aspects of the business which has already demonstrated potential cyber-attacks. (Katharina Rick et al, 2016).
- CIO magazine in their “2015 State of the CIO survey" have publicized that nowadays Chief Information Officers typically spend nearly one third of their time issues related to cybersecurity. One of their top four priorities happened to be cybersecurity. Information Sharing And Collaboration (CIO.COM, n.d.).
- Allan, K et al. suggests that the next level of cybersecurity within the Oil & Gas sector would be to use working groups to share and publicize threat intelligence and to use the experience to drive change and improvement programs. (Allan, K., & Sutton, S, 2015). They also add that the leveraging security-vendor technology would help to reinforce various aspects of cyber threat monitoring, alerting, defense and response. (Allan, K., & Sutton, S, 2015).
- Denise E. Zheng and James A. Lewis recommends that sharing information is essential for better cyber incident detection. This also reduces duplication of efforts. (Zheng, D. E., & Lewis, J. A, 2015).
- Nolan in his report on “Cybersecurity and Information Sharing: Legal Challenges and Solutions” scrutinizes several issues that are legal in nature and result from sharing of the cybersecurity intelligence. Primarily he focusses on two clear areas. i.e. sharing cyber security information within the custody of (i) government organizations and (ii) private sector. (Nolan, A, 2015).
- Oil and Natural Gas Information Sharing Analysis Center ONG-ISAC nurtures collaboration with Oil & Gas companies and government bodies by sharing insightful information on cybersecurity incidents, dangers, weaknesses and allied responses in the O&G sector. (ONG-ISAC, 2016).

- Velda Addison reports that though the Oil & Gas industry is constantly under cyber-attack, the culture of information sharing is very poor. This is as per the security experts speaking at the annual conference of American Petroleum Institute (API). (Velda Addison, 2015). Since the incident in one organization may be the responsibility of the industry, there is a significant requirement to share information among a community. (Velda Addison, 2015).
- Chris Jonson et al in their “Guide to Cyber Threat Information Sharing” as part of NIST Special publication says that cyber-threat information is the type of information which can help an organization to detect, gauge, observe, and counter the cyber threats. (Johnson, C. S et al., 2016) This also incorporate signs of compromise; methods, practices and procedures which are used by the threat actors; This further extends to recommended tasks to detect, hold, or thwart the attacks; and not the least the conclusions from the investigations of the incidents. Organizations who generally exchange the information on cyber threats with others are said to enhance their own security stances as well as others. NIST provide recommendations for launching and joining in an eco-system for sharing cyber threat realted information. These reccommendations aids companies institute goals on information sharing. The guidelines would also regulate the publication and dissemination of threat related information, involve the present sharing groups, and make efficient use of threat releated information in aid of company’s high level cybersecurity exercises. (Johnson, C. S et al., 2016).

3.5.9 Science of Cybersecurity

3.6 Theoretical Constructs

A self-governing group called JASON is a group of elite scientists who advises the United States government on matters of science & technology, mostly of a delicate nature. The US Department of Defense (DoD) requested the JASON group to critically scrutinize the theory as well the practice associated with cyber-security. Also they were requested to evaluate if any underlying fundamental principles that can make it possible to accept a better scientific approach. The aim was to identify the requirement in creating new science for cyber-security, add on to suggest specific ways by which scientific techniques can be applied in this subject. (JASON, The Mitre Corporation, 2010). The research paper looks at the “science” behind cybersecurity.

The report highlights the challenge in building a theoretical construct. Cyber-security being an artificial construct has meant that there are very few a prior constraints on either the attackers or the defenders. The above said challenges are further multiplied by the dynamic nature of the threats correlated with cyber-security the response. Thus there is not a single area of science that would comprehensively address the entire salient issues.

Cybersecurity as a domain which is not in its beginning and does not have a theoretical grounding like other areas. The authors look at compare various domains from economics to agriculture to cybersecurity to observe the similarity and difference. They concluded community of researchers are unable to reproduce the results and reuse the result and cybersecurity is essentially an applied science.

3.7 THE GAME OF CYBERSECURITY

Network security has been a popular domain with Game Theory researchers with Liang and Xioa, (Liang & Xiao, 2013 Hespanha (Hespanha, 2002). and Luo et al. (Yi Luo, 2010). They have looked at various components of network security. The biggest criticism of the Game theory centric approach is that does not consider realistic attack scenarios and the complex computational models that serve as a warning. (Roy, et al., 2010).

Laudon and Trever’s 4 Layer propose a 4 layer cybersecurity model for the e-commerce sector includes Data Protection, Technology, Organization Policies and Procedures with Laws & Industry standards forming the outermost concentric circle. (Laudon & Trevor, 2015). All the four layers are relevant in the context of the Oil & Gas industry as well. However, the Oil & Gas industry also brings with it the Information Sharing and Communication which does not play a role in the e-commerce world.

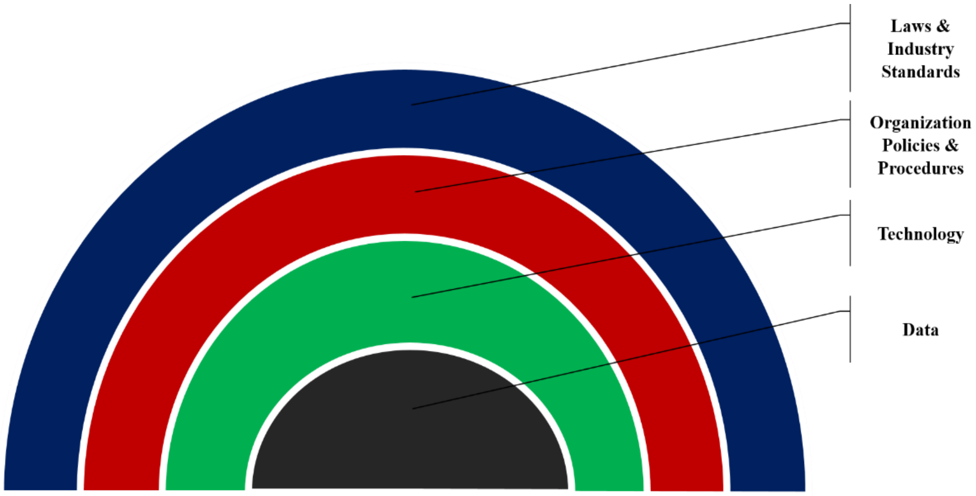


Figure 0-1 Laudon and Traver 4 Layer Model for Cybersecurity

3.8 LITERATURE REVIEW SUMMARY

It is apparent from literature review that there are several variables that enhance the cybersecurity in the Oil & Gas industry. However, there is no available literature on the factors that contribute cybersecurity in the Indian Oil & Gas industry. This research paper endeavors to address the void in the research.

3.9 VARIABLES EMANATED AFTER LITERATURE SURVEY

After the literature survey, 21 variables have emanated, which form the basic constituents of Cybersecurity in Oil & Gas industry. Table 3.6 lists the emanated variables.

Table 0-1 Variables Emanated from Literature Survey

Definitions of variables		
S.No	**Variables**	**Remarks**
1	Baseline Risk Assessment	Oil & Gas industry should conduct a baseline cybersecurity risk assessment and arrive at a risk score.
2	Periodic Cybersecurity Drills	Periodic Industry wide cybersecurity drills should be conducted in the Oil & Gas industry.
3	Third Party Security Assessment	Third party security assessments should be made mandatory on an annual basis in the Oil & Gas industry
4	Cybersecurity Assessment Review	Cybersecurity risk assessments should be reviewed periodically
5	Inventory of Cyber-physical Assets	Organization should identify and maintain an inventory of its critical cyber-physical assets.
6	Certification of Products	There is a need to enforce security certifications of products that are categorized as critical cyber-physical assets.

7	Logging of Changes in Cyber-physical Assets	Every change to the cyber-physical assets should be logged.
8	Identity Management	Provisioning and de-provisioning of identities to the entities followed by creating and maintaining them. (When someone quits the organization, identities need to be removed.)
9	Credentials Management	Periodical review of credentials is essential to confirm that they are related with the right person or right entity
10	Revoking Access	Access to cyber physical assets should be revoked when no longer required.
11	Collect Information from Industry Associations	Collection of useful information from dependable sources like industry associations, CERT etc for threat identification and correlated responses.
12	Analyze Vulnerability Information	Collection and analyzing of vulnerability information using scanning tools, security tests using penetration techniques to minimize cybersecurity vulnerabilities.

13	Threat and Vulnerability Management	Stakeholders should be identified and involved for threat and vulnerability management activities
14	Collaboration Forum for Info Sharing	There is a need to set up an Oil & Gas industry specific collaboration forum to share security knowledge, incidents and best practices
15	Disclosure to Nodal Agency	Disclosure of breaches and security incidents to a nodal agency should be made mandatory for companies in the Oil & Gas industry.
16	Directory at Nodal Agency	It is important for the nodal agency to main a current directory of industry wide cybersecurity emergency response contacts
17	Responsible Senior Executive	Organization should identify and nominate a senior executive (like Chief Information Security Officer - CISO) who would be reporting to the Board.
18	Training	Cybersecurity education and training should be made mandatory for all employees in the Oil & Gas industry

19	Employee Screening	Employees working in and also having admission to secured domains should be screened and security cleared.
20	Cybersecurity Program Strategy	Every organization comes out with a strategy for cybersecurity program that comprise of the cybersecurity objectives and an execution methodology.
21	Executive Sponsorship	Sponsorship is important for implementing the cybersecurity program for providing resources like People, Tools and Funding.

3.10 Key Gaps in Literature

3.10.1 Research Gap

Indian Government, in order to protect the CIIs in India, elected ‘National Crucial information Infrastructure Protection Centre’ (NCIIPC) which belongs to National Technical Research Organization (NTRO) to be the nodal agency. This comes under the Section 70A(1) in the Information Technology (IT Amendment) Act in the year 2008. (NCIIPC, 2014). This will also encompass all measures including correlated Research & Development. With an intention to protect and watch constantly the information and fortify defenses from cyber-attacks, the National Cybersecurity Policy 2013 was published on 2nd July, 2013 by the Indian Government & the Guidelines for Protection of National Crucial information Infrastructure by NTRO. (NCIIPC, 2014).

The UK government research report on cybersecurity standards points out that there are over a 1000 publications globally that relate to cybersecurity in one form or other (Department of Business Innovation & Skills, 2013). A big challenge in the cybersecurity domain is the oversupply of guidelines, standards and frameworks on security which will be very difficult to customize to the organizational needs.

The literature survey established the lack of domain specific regulations for the Indian Oil & Gas industry. A focused domain specific regulation for the Indian Oil & Gas industry would help the organizations to focus on one single standard meant for the country.

3.10.2 THEORETICAL GAP

Cybersecurity is a nascent domain and the theoretical frameworks are yet to be established. The complex and diverse nature of the cybersecurity world has meant that there is no simple theoretical fix from either the mathematical, science or other areas. The existing endeavors to provide a theoretical model are mainly complex and involve significant computational work. There is no equivalent of the Laudon and Trever 4 layer E-commerce security model in the cybersecurity domain. The researcher could not find equivalent of the Laudon & Trevor 4 layer cybersecurity model for the Oil & Gas industry. Though there is an ONG C2M2, the researcher could not find Indian equivalent of the model in the cybersecurity domain for the Oil & Gas industry.

3.11 CONCLUDING REMARKS

The survey doen by the researcher helped to identify the vulnerabilities in the cybersecurity space of National Critical Infrastructure across the globe and India. It has been found that the enrgy sector is one if the prime targets for the cyber-attackers. From the survey it was concluded that the governing interventions and mandates are needed to improve the cybersecurity posture. The literature survey covered how advanced countries like US and UK have taken efforts in bringing regulatory interventions.

The survey idnetified that the cybersecurity in in the nascent stage and there is no cybersecurity model such as Ladon-Trevor 4 layer model for the Oil and Gas industry

4 RESEARCH DESIGN

4.1 OVERVIEW

“Research Design is defined as the blueprint that details out how the researcher intends to achieve his end objective”. A major component of research design is the research methodology, the approach to collection, measurement and interpretation of data. Research design has to consider the research strategy and research philosophy. The former deals with whether Qualitative or Quantitative or Mixed methods research would address the research objectives and the latter answers the question on choice of epistemology and ontology. This chapter also recognizes the research objectives, the research questions and the proposed strategy to address these questions. It details out the qualitative research strategy that is proposed to answer the first research question and the quantitative research strategy that addresses the second research question. The chapter delves into the rationale as well as the theoretical framework to justify the choices made at the various points in the research framework. Lastly, the chapter includes the metrics and thresholds to establish the reliability in addition to the validity of the research design.

4.2 INTRODUCTION

The research design offers an outline for data gathering and data analysis. (Bryman & Bell, Business Research Methods, 3e, 2011). It reflects the choice of priorities that the researcher makes to

- Express causal connection between variables
- To generalize the result of the investigation to a larger group than those who were studied during the examination
- Comprehend the behavior and its significance in certain context
- Have an appreciation of a social phenomenon in the current context

Research design is essentially a planned outline for the data gathering, data measurement and data analysis.

Research design has a number of components (Kothari C, 2013).

- Sampling design or the method of selecting items that are to be part of the study
- Statistical design or the details on the sample size, frequency and analysis of the data gathered
- Operational design or the execution of the research

The research design needs to consider the means of obtaining the information, the objective and nature of the problem, and the practical issue of the resources – including time and money that are available with the researcher to perform the research.

Categories into which research design can be broken into include:

1. Exploratory research is aimed at formulating the problem for detailed investigation or to develop a working hypothesis.

2. Descriptive & Diagnostic Research is concerned with describing the characteristics of the subject being investigated or aims to establish a causal relationship.

Exploratory research focusses on the discovery of new ideas, and the research design therefore needs to be flexible to accommodate less precise or broad definition of the research problem at the initial stage, which would evolve into a more precise meaning throughout the research process. Exploratory research design typically involves one of the following three approaches.

1. **Literature Review** – that involves a detailed analysis of the existing literature on the domain to understand the current body of knowledge on the subject. This will help and help formulate the hypothesis for the proposed research.

2. **Experience Survey** – that involves surveying people who have a practical experience on the subject
3. **Analysis of thought provoking example** – that involves intensive study of the phenomenon of interest.

Descriptive Research and Diagnostic Research are more rigid, prevent bias and ensure reliability. The design must focus on

- Formulating the objective
- Defining the data collection methods
- Defining the sample
- Collecting the data
- Data Analysis
- Conclusion

4.3 RESEARCH STRATEGY

Research Strategy can be classified as **Quantitative and Qualitative**. At a superficial level, the two differ in that quantitative research involved measurement while qualitative research does not involve measurement. (Bryman & Bell, Business Research Methods, 3/e, 2011). There are fundamental differences with different epistemological and ontological considerations.

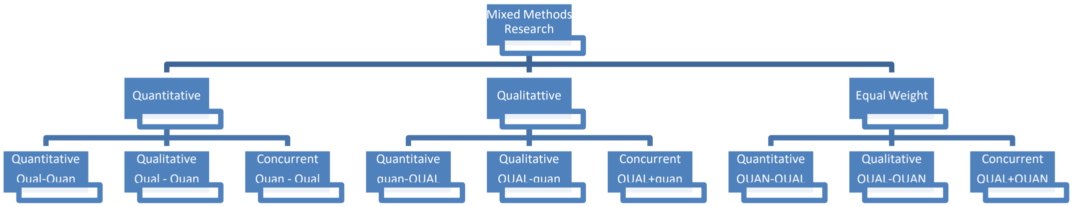


Figure 4-1 Classification of Mixed Methods Research

Quantitative Research Strategy highlights the quantification in data gathering data analysis and necessitates a logical approach. It mostly focuses on testing of theories. It embraces positivism and observes social reality as an outward and objective reality. The principal orientation of quantitative research with respect to the part of the theory in relation to research is more logical.

Qualitative Research Strategy underlines words as opposed to quantification and is predominantly inductive in approach to the association between the theory and the research. This research discards positivism and views social reality as a persistently moving property of individuals' creation. The principal orientation of qualitative research with respect to the part of the theory in relation to research is more Inductive.

While the above characteristics are generally true, there are exceptions. Apart from that, Qualitative and Quantitative Research also have different philosophical orientation.

In a **Mixed-Methods Research,** both the two research strategies articulated Qualitative and Quantitative co-exist. Mixed Method approach to business research has gained popularity and a plethora of research scholars have adopted mixed-method research. Mixed method research can be classified based on (i) Priority and (ii) Sequence. Thus, Mixed-Methods Research can potentially have nine different approaches. The research can either have Quantitative, Qualitative as priority or both could have equal weight. The second level of the classification is on the sequence of qualitative or quantitative or both of these can be done concurrently. All the options are captured in the Figure 4.1 above and the choice of priority and sequence employed in this research is highlighted in red. The capitals highlight the priority, while a '+' sign indicates concurrent research.

In this research the qualitative analysis is executed first using the Framework Analysis with the objective to understand the cybersecurity challenges in the Oil and Gas industry to answer the first research question. This the detailed quantitative analysis using Exploratory and Confirmatory Factor Analysis is performed to answer the central research question.

4.4 RESEARCH PHILOSOPHY

Epistemology answers the question on what is knowledge is acceptable in a discipline. The central issue is whether social sciences can be learnt occurring to the same principles and procedures as handled in natural science. The position that promotes the usage of the principles of natural sciences to understand social reality is referred to as “Positivism”. The contrasting view, that some researchers passionately advocate is that social reality is fundamentally different from natural science and therefore would require an alternate approach to study social behavior. This is termed as “Interpretivism”. (Bryman & Bell, Business Research Methods 3/e, 2011).

Ontology deals with the nature of social reality. An Ontological position that holds that the social phenomenon and their implications are independent of social actors is Objectivism. The alternate view or Ontological position is called as Constructionism or Constructivism. (Bryman & Bell, Business Research Methods 3/e, 2011). Proponents of constructivism argue social happenings and their connotations are persistently being achieved by the social actors. Social phenomena and their groups are formed by social collaboration and are in constant change.

In conclusion, business research is impacted by many factors that is shown in Figure 4.2 including Theory, Epistemology, Ontology, Values, and Practical consideration. The initial step of any business research is to define the research problem.

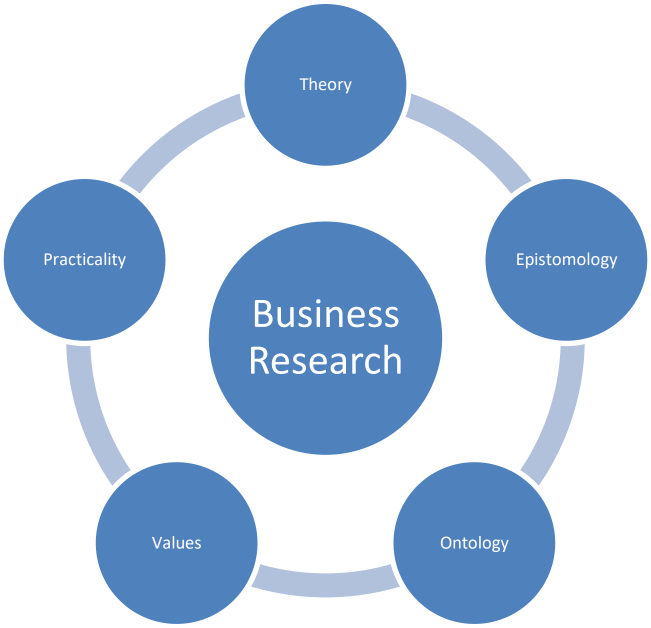


Figure 4-2 Influence on Business Research

4.5 RESEARCH PROBLEM

The research problem arises from the research gap in the literature review. The gaps that were identified in the continuing chapter are:

- The lack of domain specific regulations for the Indian Oil and Gas industry.
- Cybersecurity is a budding domain and the theoretical frameworks are yet to be established. Laudon and Trever define a 4 layer model for security in the ecommerce sector. The core of the 4 layers is the "Data" and the other layers are technology, organizational policies and procedures and Laws and Industry standards.

The research problem for the study is therefore:

"To adapt the 4 layer Information Security framework to identify constituents of the cybersecurity mandate for the Indian Oil and Gas industry."

After identification of the Research Problem, the next step is to articulate the Research Questions from the Research Problem.

4.6 RESEARCH QUESTIONS

Taking into considerations of the above discussions, the following research questions arise:

Research Question 1

1. *What are the cybersecurity challenges in the Indian Oil and Gas industry?(RQ1)*

Research Question 2

2. *What are the relevant factors that enhance cybersecurity and their significance in the Indian Oil and Gas industry? (RQ2)*

The purpose of RQ2 is to determine the relevant cybersecurity factors and establish their significance in the Indian Oil and Gas industry. However in terms of sequencing, the study first focused on eliciting the cybersecurity challenges that affect the Indian Oil and Gas industry and subsequently identifying the factor and their relevance to the industry. The Research Questions lead to the Objective of the Research.

4.7 RESEARCH OBJECTIVES

Built on the research questions, the following research objectives are formulated:

Research Objective 1

1. *To discover the cybersecurity challenges in the Indian Oil and Gas industry (RO1).*

Research Objective 2

2. *To determine the relevant factors that can enhance cybersecurity and test their significance in the in the Indian Oil and Gas industry? (RO2)*

4.8 Research Design to address Research Objective 1

As discussed in the previous section, this research study utilizes mixed methods research with a priority on quantitative techniques and a sequence of qualitative research followed by quantitative research. Table 4-1 articluates the research design choices to address Research Objective 1.

Table 4-1 Research Design Choice to address Research Objective 1

Components	Choices in the Research
Research Design	Exploratory Research
Research Strategy	Qualitative Research
Principal Orientation to the role of theory	Inductive
Epistemology	Interpretivism
Ontology	Constructionism

The Qualitative Research Strategy as discussed propose a sequential approach to undertaking qualitative research as show in Figure 4.3 below.

The research starts with the general research question which in this research is to discover the cybersecurity challenges in the Indian Oil and Gas industry which has the following sequential steps:

- Selecting the relevant subjects and site(s)
- Appropriate data collection
- Data interpretation
- Abstract and theoretical work
- Writing up of the research findings and the conclusions

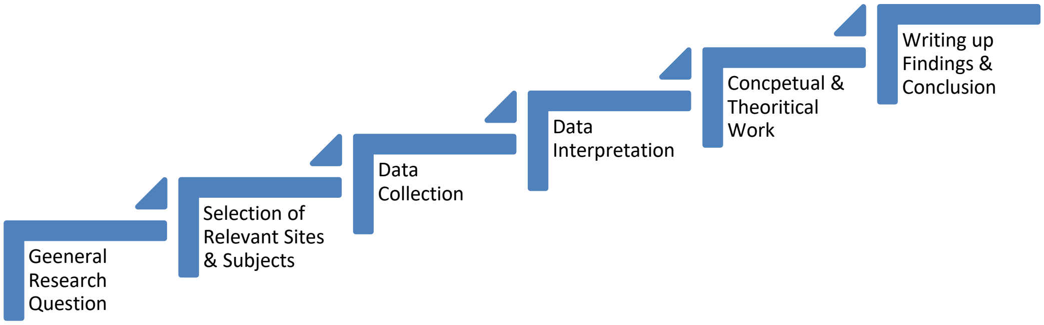

Geeneral Research Question
Selection of Relevant Sites & Subjects
Data Collection
Data Interpretation
Concpetual & Theoritical Work
Writing up Findings & Conclusion

Figure 4-3 Outline of Qualitative Research Steps

Each of the steps involved in the Qualitative Research are discussed in detail below

4.8.1 Selection of Relevant Sites & Subjects

The extent or the site of this study is India. The respondents or subjects are drawn from the universe of Policy makers of the government across both the Indian Oil and Gas industry and the cybersecurity domains, members of the office of the National

Security Advisor (NSA), service providers and suppliers from both the Oil and Gas and Security industry.

4.8.2 APPROACH TO SAMPLING AND SAMPLING SIZE

Qualitative research sampling often involves **purposive sampling**. Probabilistic sampling is not appropriate in qualitative analysis. (Bryman & Bell, Business Research Methods 3/e, 2011). It is recommended that sampling be continued till Theoretical Saturation is attained. Theoretical Saturation indicates that consecutive interviews and observations have shaped the basis for the formation of a group and established its importance. Theoretical saturation is identifiable if no relevant data surface, the category itself is well developed and the relationships between the categories are established. (Bryman & Bell, Business Research Methods 3/e, 2011).

4.8.3 GATHERING OF RELEVANT DATA

The Interview is the most widely employed method in qualitative research for collection of data. In-depth Interviews is "repeated head-on encounters between the researcher and informants with the ultimate goal of understanding the informants' perspectives on their lives, experiences or situations as expressed in their own words". (Minichiello, V et al., 1990). & (MacDougall, C., & Fudge, E, 2001).

The various characteristics of qualitative interview as:

- Qualitative interviews are focused more on the greater generality in the creation of the interviewees' perspectives which causes them to be less structured in nature.
- The interviewers have a greater degree of freedom and an depart from the scheduled guide and if required interview the subject multiple times
- The qualitative interview are more flexible and the researcher's interest is in elicitation of rich and detailed answers

Two major types of interviews are identified. The two major types are unstructured interviews and semi-structured interviews. In the latter, the researcher formulates a list of questions on specific topics that is used to guide the researcher through the interview; it is referred to as the Interview Protocol. Largely, the questions with similar wordings are asked across all interviewees, while still retaining the ability to adjust based on the respondent's answer. The Interview Protocol is series of memory prompts, questions or visual cues that enable the researcher to glean the ways in which the respondents view their social world.

The questions or the cues in the Interview Protocol is the outcome of literature review, including the review of the global experience from cybersecurity regulations / standards in the Oil and Gas industry and the initial short list of variables that emerged from the literature review.

4.8.4 VALIDATION

A semi-structured interview was conducted to finalize the list of variables by subjecting it to the respondents till data saturation happened (Appendix 7.1). The enclosed questionnaire was sent to the 1st respondent and based on his/her inputs, the questionnaire was modified. Thereafter it was delivered to the 2nd respondent and the same process was followed till the saturation of the variables occurred.

- The interviewees were briefed about the the intention and the duration of the interview
- Each interviewees gave his or her informed consent
- An interview guide was developed that listed the questions explored during the course of the interview

Process – potential interviewees were initially contacted; a date was mutually decided for subsequent interview for those who agreed to participate. On the agreed date, the interview was conducted. Interviews were semi-structured and were conversational and the questions standardized. Key data points were summarized immediately following the interview.

The following **three variables** were eliminated based on the responses of the respondents.

- **Consumption Data Records** - Detailed fuel consumption records that are available from the fuel retail outlets.
- **Data Retention Guidelines** - Data lifecycle requirements that identify the data types and duration for retention, storage and purging.
- **Financial Penalizations**- Fines and penalties for loss of customer sensitive data if any.

4.8.5 Interpretation of Data

Coding is the principal pace in the analysis of data in qualitative research and is a well-established principal. (Bryman & Bell, Business Research Methods 3/e, 2011). A 5 step "Framework Analysis" process for analysis of the qualitative data for applied policy research, which aligns perfectly to the requirements of this research is generally used. The 5 step Framework Analysis is described and represented in the Figure 4.4 below.

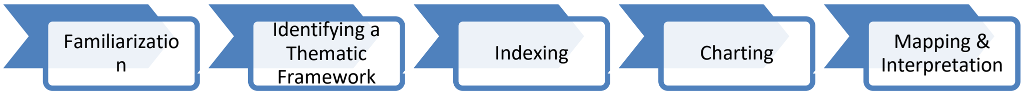


Figure 4-4 Ritchie and Spencer Framework Analysis

- Familiarization: essentially involves the immersion in the data to identify recurrent themes and list key ideas.
- Identifying a Thematic Framework: This step involves finding the key issues, concepts, patterns or themes in the data that can be used to sift or sort the data. Building the thematic framework involves logical and intuitive thinking.

- Indexing: an approach in which data is labelling and sorted into manageable chunks to be used for subsequent retrieval and exploration
- Charting: involves building the big picture view from the themes identified and involves abstraction and synthesis of the gathered data.
- Mapping and Interpretation: involves pulling together the key components of the data into a whole to define concepts, mapping range of phenomena, finding association and developing strategies etc. that is mapped to the fundamental intent of the study

4.8.6 RESEARCH DESIGN OBJECTIVE 1 – SUMMARY

The summary of the research design to address objective 1 is captured in Table 4.2 shown below. It highlights the execution approach and choices made at various points in the qualitative research sequence and provides an overview of the entire research design.

Table 4-2 Execution Approach & Choice of Research Design to address RO1

	Sequence of Steps in Qualitative Research	Execution Approach used in this research	Choices made in the research
1	General Research Question		
2	Selecting relevant sites(s) and subjects	**Sampling:** Purposive, Non-probabilistic Sampling	CIOs, CISOs, Service Providers, Policy Makers in the Indian Oil and Gas industry and Security domains

		Sample Size: Theoretical Saturation	
3	Collection of relevant data	In-depth Semi-Structured Interviews with a pre-defined Interview Protocol	
4	Interpretation of Data	Ritchie & Spencer Framework of Analysis	Leveraging Atlas TI for coding, formulating of themes, charting and interpreting.
5	Conceptual and Theoretical work	Focus on identifying the cybersecurity challenge in the Oil and Gas industry	
6	Writing up Findings / Conclusions	To address Research Objective 1	I. Cybersecurity challenges in the Indian Oil and Gas industry I. Final Set of Variable for as

			input for Research Objective 2

4.9 Research Design to Address Objective 2

The choice of research design to address objective 2 is articulated in the Table 4.3 below. Objective measurements and statistical analysis of data are collected using computational techniques. Quantitative methods focus on these analysis. It gathers the numerical data and takes a broad view of the data across groups of people and explains a particular phenomenon. (Babbie, 2010).

Table 4.3 - Choice of Research Design to address Research Objective 2

Components	Choices in this Research
Research Design	Descriptive Research
Research Strategy	Quantitative Research
Principal Orientation to the role of theory	Deductive or testing of theory
Epistemology	Positivism
Ontology	Objectivism

A multi-stage process to address quantitative research is shown in 7-8 below. (Bryman & Bell, Business Research Methods 3/e, 2011). The hypothesis for the research flows from evaluating the theory or reviewing the literature. On occasion it is likely that in the place of the hypothesis, the theory acts loosely as a set of concerns in relation to the hypothesis.

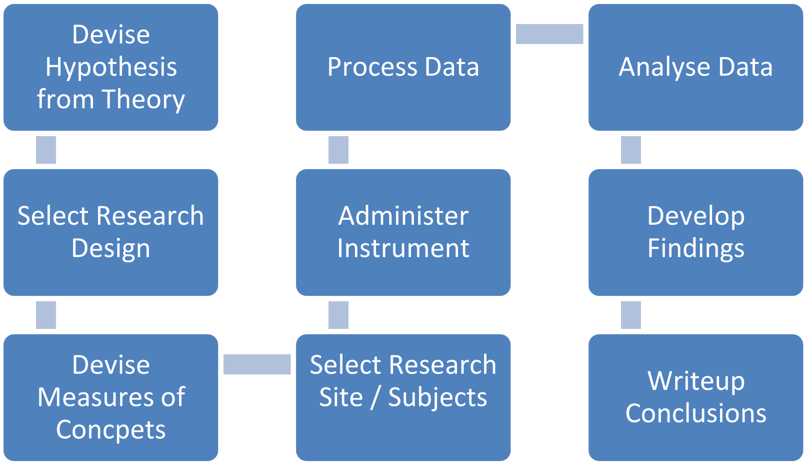


Figure 4-5 Quantitative Research Methods

4.9.1 Select Research Design

There are a number of choices of Research design in quantitative research – Cross-Sectional Design, Experiment, Quasi-Experiment, and Longitudinal Design. The **Cross-Sectional Design** necessitates both the collection of quantitative and quantifiable data at a single instance of at least two variables which are then inspected to detect associated patterns.

Survey Research comprises of a cross-sectional design of data collection with questionnaires or structured interview. The choice of research design has a direct bearing on the measures of validity and interconnection.

4.9.2 Devise Measures of Concepts

Concepts are the basis of theory on which business research is conducted. Concepts are groups for the organization of ideas and observation. (Bulmer, 1984) & (Bryman

& Bell, Business Research Methods 3/e, 2011). Quantitative research thrives on measurement of concepts. **Measures** allow fine differentiation, provide a consistent yardstick and provide a basis for a precise measurement of the degree of relationship between the concepts. Measures are used for things that can be unambiguously counted like age, salary or turnover. **Indicators** are used to "stand in" for the concepts that are less directly quantifiable like job satisfaction, performance, intelligence etc.

Measurements become challenging when the concepts to be measured are complex, abstract and when there is no standardized measurement tools. **Scaling** enables the researcher to measure abstract concepts. Scaling is when various degrees of attitude, opinion or other concepts are assigned a numerical score. The scale is continuous and is comprised of the highest point, the lowest point and multiple intermediate points between the two extremes.

4.9.2.1 Choice of Scale – Likert Type Scale

Likert-type scales are developed using item analysis approach. This kind of scale comprises of numerous statements that either express a positive or negative attitude towards a particular subject. The variables identified as part of the qualitative analysis was converted in the form of question with an option to choose a response. The respondents were asked to select the choices between agreement or disagreement with statement on a 5-point scale with varying degrees of agreement or disagreement. The Likert scale is shown in Figure 4.6 below.

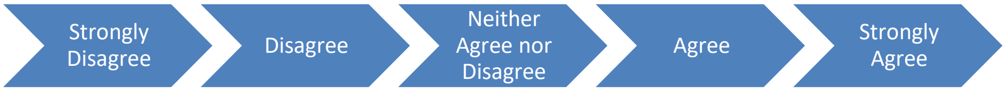


Figure 4-6 Likert Type Scale

The Likert-type scale is advantageous to other scales in that it is relatively easy to make, it is reliable and is frequently used in opinion research. Likert-type scale suffers from the constraint of being only an ordinal scale, but is a very popular research tool. The variables determined from the qualitative analysis as part of research design one formed the input for the Likert-type scale. (Kothari C. R., 2013).

4.9.2.2 Testing the Instrument

Pilot Testing - The questionnaire was pretested by administering it to 30 respondents. This resulted in rewording of few questions to remove ambiguity and bring in clarity before the questionnaire was administered again.

Reliability - Reliability describes the consistency of a measure of a certain concept. (Bryman & Bell, Business Research Methods 3/e, 2011). Reliability of an instrument is measured using multiple parameters – **Internal Reliability**, Inter-Observer Consistency, and Stability. Of this Internal Reliability, which is the "measure of whether or not the indicators that make up the scale or index are consistent", is most often used to validate the reliability of the instrument. **Cronbach's alpha** is widely used to test internal reliability. A computed Cronbach's alpha co-efficient would vary from 0 (or no internal reliability) to 1 (to denote perfect internal reliability). As a general rule, a Cronbach's alpha score of 0.7 or above is deemed as an acceptable score. (Schutte, Toppinnen, Kalimo, & Schaufeli, 2000).

Validity - Validity of a measurement deals with weather or not the measure of the concept truly measures the concept. Validity of instrument can be measured in multiple ways. Face Validity or Construct Validity which includes both Convergent and divergent Validity. We discuss the face validity in this section and other measures are discussed in the subsequent section on Confirmatory Factor Analysis.

Face Validity is a subjective process where the experts in the field are asked to judge whether or not the measure reflects the concept concerned. In this research the questionnaire was administered to 30 respondents with experience in the cybersecurity domain and in the Indian Oil and Gas industry to establish the face validity of the instrument.

4.9.3 Selection of Research Sites and Subjects

The research site for the research was India and the subjects or respondents were similar to the audience in the qualitative research that included a mix of policy makers from both the Oil and Gas domain, academics, CIO’s, CEO’s , Oil Field Service providers, EPC, Security Service providers, System Integrators, Government bodies, Independent bodies, Academic Institutions, Research Institutions and Analysts. From within the Oil and Gas industry, the selection of people was taken from across the entire value chain from Downstream, Midstream and Upstream segments.

4.9.4 Approach to Sampling

Probabilistic sampling techniques are most popularly associated with quantitative analysis. “Probability sampling is defined as the sample that has been randomly selected in a process that ensures that each unit in the population has a known chance of being chosen.” (Bryman & Bell, Business Research Methods 3/e, 2011). A probability sample is assumed to be a sample which is illustrative of the entire population. The popularity of probability sample stems from the fact that it is possible to make inferences or generalize the findings on the population using the information gathered from a random sample that was drawn from the identical population. (Bryman & Bell, Business Research Methods 3/e, 2011).

The research employed **Stratified random sample** across three different criterion

- Decision Makers - Policy Maker / Government Sector / Academician
- Leaders of the Oil and Gas Industry - CIOs, CISOs
- Practitioners - IT Managers
- Facilitators - System Integrators - Security professional - Security Auditor

Fig 4.7 shows the value chain wise distribution of the above respondents. Sample Size –305 respondents responded the questionnaire.

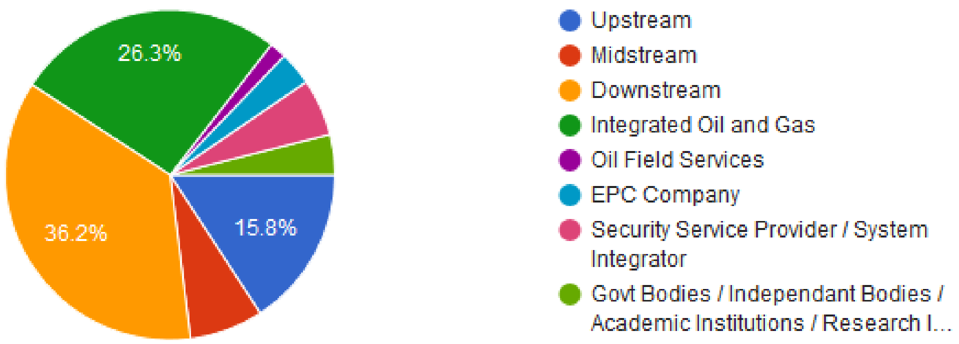


Figure 4-7 Distribution of Respondents Value Chain wise

The sample profile of the respondents for the value chain is given below in Table 4.4.

Table 4-3 Profile of the Survey Respondents

Stream	**Profile of the respondents**
Upstream	• Deputy General Manager (Production), ONGC • Senior Production Engineer- Upstream, Vedanta Ltd • Lead - IT security and Compliance, Cairn India • Sr.Mechanical Engineer, Cairn India • Production Engineer, Cairn India

	• HSEF Management, Cairn Energy • Smart Application Specialist, Shell India • Engineering Information Management Consultant, Shell • Senior Engineer, Reliance Industries • Lead Engineer, RIL E & P • Central Planning Engineer, Reliance • Subsea Engineer / Planning Engineer, Reliance Industries
Midstream	• Crude Scheduling professional, Essar Oil • Manager, Indraprastha Gas Limited
Downstream	• Executive Director, IOCL • Executive Director, BPCL • Executive Director, HPCL • Project Manager, Bharat Oman Refineries Limited • Manager, Chennai Petroleum Corp. Ltd, IOCL • Chief General Manager (Technical), IOCL • General Manager (HS&E), ICOL • Vice President, Reliance • Vice President - Process Automation, Reliance Industries • Head - Central Technical Services, Reliance Industries • Manager, Reliance Industries Ltd • Head IT, Essar India Limited

	• Deputy Manager, HPCL-Mittal Energy Ltd • Refinery Process Engineer, HPCL Mittal • Deputy Manager, Essasr Oil • Engineer, HPCL-Mittal Energy Limited • Manager, ONGC petro additions Limited • Vice President, Indian Oil Sky tanking Pvt. Ltd. • Territory Sales Manager, Essar Oil • Deputy Manager-IT, HPCL-Mittal Energy Ltd • Maintenance Manager, IOCL • Assist. Manager-MES/IOT & Integration at HMEL • Assistant Manager, HMEL • Sales Manager, Essar
Oil Field Service Companies	• SAP Technical Lead, Schlumberger • Consulting Geologist, Halliburton • HSE Advisor, Hardy E & P (I) • HC Accounting / Energy Components Professional, Applus Velosi • Advisor refinery process, Technip India Limited
Security Service Provider / System Integrator	• Real Time Data Management & Industrial IoT Consultant, Wipro • Business Analyst, Cybage Software • Lead Subject Matter Expert (O&G), Rolta India

	• Senior Project Manager, AspenTech India • Senior SAP FICO/SD/MM Consultant, Consulting Organization
Government Bodies / Independent Bodies Academic Institutions / Research Institutions	• Joint Director (IT), Petroleum Planning and Analysis Cell (PPAC), MoPNG • Director, Centre for High Technology, New Delhi, MoPNG • Cyber Dispute Risk Management Consultant • Independent Oil and Gas Consultant • Executive, National Cyber Safety and Security Standards • Consultant for Safety Audits / Risk Assessment

This ensured that there was a balance of opinion across the various sections of the population of interest. The other aspects of sampling to be considered are:

Sampling Frame - or all the units of the population that would be the source of the sample. This consisted of the stakeholders who have a major role in cybersecurity of the Indian Oil and Gas industry. Th sampling frame identifies over 1000 respondents across the four strata.

Sampling Element - As the survey was aimed to elicit feedback on cybersecurity for the Indian Oil and Gas industry, the sampling element was described as the set of people who were engaged in policy decision making, the middle or senior management in the Indian Oil and Gas industry or service providers.

Extent: or the location of the data collection was limited to the Indian geography

4.9.5 APPROACH TO SAMPLE SIZE

The decision on the Sample size depends on a number of considerations – precision required and constraints of time and cost. An increase in the sample size would result in the decrease in the sampling error; therefore a higher precision would require a larger sample size. Yamane's formula provides guidance on the sample size needed for the research. (Yamane, 1967).

$n = N \,/\, 1 + N.e^2$

Where

n = Sample Size needed

N = Size of the Population

e = Levels of Precision

Employing the Yamane, formula for a population (N) size of 1000, and a precision (e) of +/- 5% would result in sample size (n) of 286.

The Sphericity test of Bartlett is able to test two hypotheses namely, that the correlation matrix is an identity matrix or that the various variables are uncorrelated. This hypothesis needs to have the significance value lower than the alpha level of the test, to reject the hypothesis and establish that there is a correlation in the variables and that the data is appropriate for factor analysis. (Lalanne, n.d).

Also the KMO measure aims to establish the adequacy of the co-relation but uses a different approach. The **KMO index** removes the effect of remaining variables to measure the relation between two variables, a partial correlation method. The KMO index then compares two values: the values between those of the partial correlations and the values of correlations between the variables. The KMO index closer to 1 would suggest that the factor analysis can act efficiently and a low KMO closer to zero would suggest that the factor analysis is not relevant (Lalanne, n.d). The KMO index can be refined further a score of 0.90s can be considered as 'marvelous', while 0.80s would be ‘meritorious’, 0.70s would be ‘middling’, 0.60s are considered as ‘mediocre’, and below .5 are ‘unacceptable’.

Given the wide range of opinion on the sampling size, this research adopts the Sphericity test of Bartlett and the KMO measure of sampling adequacy to establish the adequacy of the co-relation matrices for factor analysis. The sample size of **305 respondents** was used in this research.

4.9.6 ADMINISTER THE INSTRUMENT

The questionnaire was divided into seven sections – section 1-6 with groups of questions aligned to a similar domain. The final segment section of the questionnaire also included an open-ended question to gather additional inputs and also to identify the strata of the sample.

The questionnaire was administered to both in person and via email using the survey forms option in Google. The in person administration of questionnaire was done largely in cybersecurity conferences and relevant industry events where the speakers and session chairs are largely handpicked from the industry thought leaders and decision makers.

4.9.7 PROCESS DATA

The data gathered from the survey was processed through SPSS software for the first step of factor analysis or Exploratory Factor Analysis (EFA) and using Amos software for analysis for generating the Confirmatory Factor Analysis.

4.9.8 ANALYZE DATA

The domain of statistics that deals with the observation on many variables and how they work in combination is termed as Multivariate analysis. (Fundación BBVA, 2014) The flow chart to decide on the choice of multivariate technique is described in the figure 4.8 below. “Exploratory Factor Analysis (EFA) or often just called as Factor Analysis is a statistical data reduction technique.” EFA helps the researcher to identify how many factors are needed to best represent the original data set of variables.   In

EFA, all the identified variables are related to every factor by a factor loading estimate. Factor Analysis helps identify the variable that loads highly on only one factor and has minor loadings on all other factors. In EFA the factors are derived from statistical results not from a prior knowledge or theory, therefore factor analysis can be performed when there is no prior knowledge of the number of factors or an understanding of which variables best load onto a selected factor. (Statistics Solution, 2013).

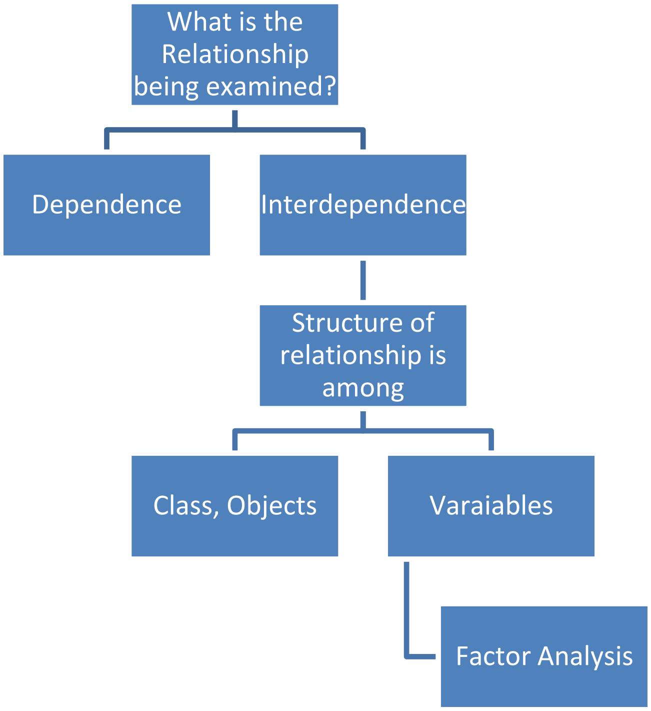

What is the Relationship being examined?
Dependence
Interdependence
Structure of relationship is among
Class, Objects
Varaiables
Factor Analysis

Figure 4-8 Classification of Multi-variate Techniques

"Confirmatory Factor Analysis (CFA) is a multivariate statistical technique, similar to EFA." Representation of measured variables with the number of constructs is taken here. But still there is a philosophical difference, in CFA the researcher uses the theory or a prior knowledge to postulate the relationship between the construct or factor & the variable.

Composite Reliability (CR)

“The Composite Reliability is defined as a measure of the overall reliability of a collection of mixed or assorted but similar items”. It differs from the reliability of individual items that is measured using Cronbach’s alpha as discussed earlier.

Construct Validity

Earlier we saw the concept face validity. Apart from this there are 2 other main measures of validity – 1. Convergent validity 2. Discriminant validity. Together they form the Construct validity. It is the level to which a test truly gauges what it claims to measure. (Messick, 1980). A test possesses Convergent validity if constructs that theoretically be related to each other are observed to be related to one another in reality. Discriminant validity is possessed, when measures of constructs that are not to be related theoretically are observed to not be related to each other in reality.

Thresholds

The thresholds for establishing reliability and convergent and discriminant validity. (Hair, Black, Babin, & Anderson, 2010) & (Gaskin, Confirmatory Factor Analysis, 2012). The threshold values are provided in the Table 4.5.

Table 4-4 Reliability and Validity Thresholds

Measure	Threshold Value
Composite Reliability (CR)	CR > 0.7
Convergent Validity	Average Variance Extracted (AVE) > 0.5
Discriminant Validity	Maximum Shared Variance or MSV < AVE

	Average Shared Variance < AVE Square Root of AVE > Inter-construct Correlations

AVE is actually a conventional measure than CR. From the results arrived out of CR itself, the researcher can arrive at a conclusion that adequate convergent validity is there, even though more than half of the variance is due to error. (Malhotra & Dash, 2011).

Evaluating Model Fit

“Model fit is generally defined by how well the chosen model correctly explains the existing correlations between the variables in the dataset”. If all the major correlations inherent in the dataset are explained by the model, it would imply a model with a good fit. Else, if there is a substantial discrepancy amongst the correlations proposed vs observed, then it leads to a poor model fit, or the proposed model does not "fit" the observed or "estimated" model. (Hu & Bentler, 1999) & (Gaskin, Confirmatory Factor Analysis, 2012).

Table 4-5 Indices of Fit

Measure	**Threshold Value**
Chi-square / DF (cmin/df)	< 3 Good. <5 Permissible
p- Value for the model	> .05
Comparative Fit Model (CFM)	> 0.95 Great, > 0.9 Traditional, > 0.8 Sometimes Permissible

Goodness of Fit Index (GFI)	> 0.95
Adjusted Goodness of Fit Index (AGFI)	> 0.8
Standardized Root Mean Square Residual (ARMR)	< 0.09
Root Mean Square Error of Approximation (RMSEA)	< 0.05 Good, 0.05-0.1 Moderate, > .10 Bad
PCLOSE	> 0.05

4.9.9 Develop Findings

The outcome of the data analysis sets the stage for interpreting the data. Developing the finding would involve validating the outcome of the analysis phase, with the original objective that was set out for the research. This could take the form of accepting or negating the hypothesis and articulating the inference of the findings. It would finally need to be tied back to the implication of the findings to the theoretical framework that formed the background for the research.

4.9.10 Research Design Objective 2 - Summary

The entire research design to address objective 2 is captured in the Table 7-6 below. It highlights the execution approach and choices made at various points in the quantitative research sequence and provides a bird's eye view of the entire research design for objective 2.

Table 4-6 Execution Approach & Choices of Research Design to address RO2

S.No	Sequence of steps in Quantitative Research	Execution Approach used in this research	Choices made in this research
1	Devise hypothesis from theory		
2	Select Research Design	**Survey Research:** Cross sectional design for data collection with questionnaire or structured interview	
3	Devise Measure of concepts	Choice of Scale: **Likert-type Scale** Testing the Instrument **Pilot Reliability Validity**	5-Point Likert scale Cronbach's Alpha Face Validity

4	Selecting relevant sites(s) and subjects	Sampling: Probability sampling, Stratified random sample Sample Size: Validated by Bartlett’s Test of Sphericity and KMO measure of sampling adequacy	CIO’s. CISOs. Service providers and Policy makers in the Indian Oil and Gas industry and Security domain.
5	Administer the Instrument	In-person or Over Email	
6	Process Data	SPSS for Exploratory Factor Analysis AMOS for Confirmatory Factor Analysis	Multivariate Analysis Exploratory Factor Analysis Confirmatory Factor Analysis
7	Analyze the data	Exploratory Factor Analysis for Data Reduction and	Identify the factor that enhance cybersecurity in

		Identifying the Factors Establish Composite Reliability Convergent Validity Discriminant Validity Good of Fit Indicator Confirmatory Factor Analysis to establish the significance	the Indian Oil and Gas industry. Use thresholds defined by Hair et al, Malhotra & Dash and Hu & Bentler. Arrive at the Best Fit model to explain the data set. Establish the significance of the factors that enhance the cybersecurity in the Oil and Gas industry.
8	Writing up Findings / Conclusions	To address Research Objective 2	Factors that enhance the cybersecurity in the Indian Oil and Gas industry and their significance.

4.10 WRITE-UP CONCLUSIONS

The culmination of the research activity is placing the report in the public domain in the form of a conference proceeding or report or journal article etc. The researcher would need to convince the readers on the robustness of the finding. The report serves one other important function. The research find would become part of the existing knowledge and serve to create a feedback loop to the first stage

4.11 CONCLUDING REMARKS

This section articulates the mixed methods research and sequence of steps for qualitative and quantitative research to address research objective 1 and 2 respectively. The qualitative research was conducted using the semi-structured in-depth interview. The literature review, the global experience and the original set of variables identified in the literature review served as the inputs for the Interview Protocol. The interviews were then transcribed and served as the data for qualitative analysis. Ritchie and Spencer's Framework analysis for Qualitative research was the framework of choice for the analysis. The five stage framework analysis has the following steps.

- Familiarization
- Identification of a thematic framework
- Indexing
- Charting
- Mapping and Interpretation

Atlas TI was the tool of choice to process the data for analysis. Qualitative analysis helped answer the first research question on the cybersecurity challenges in the Indian Oil and Gas industry.

The output of the qualitative research also helped narrow down the initial set of variables that became the input to descriptive research. The variables were the parameters administered on a 5 point Likert scale to the respondents. The process of data reduction of the original set of variables into relevant factors that enhance cybersecurity in the Indian Oil and Gas industry was achieved using Exploratory Factor Analysis. Confirmatory Factor Analysis helped establish the significance of the factors using model fit indices.

5 DATA ANALYSIS AND INTERPRETATION

5.1 OVERVIEW

This chapter on Data Analysis is the execution of the blue-print outlined in the Research Design section. It deals with the data gathering, analysis and interpretation of the data leading to the answering of the research questions and addressing the objective of the research. The initial segment of data analysis focusses on the qualitative aspects that focusses on understanding the cybersecurity challenges in the Indian Oil & Gas industry and output of the analysis helps identify the variables for the factor analysis.

The second section answers the question on the factors that enhance cybersecurity in the Indian Oil & Gas industry using Exploratory Factor Analysis and understand their implication with Confirmatory Factor Analysis report.

5.2 QUALITATIVE DATA ANALYSIS – OBJECTIVE 1

Purposive sampling or judgmental sampling is employed in this research. The CIO / COO / GMs of Oil & Gas companies, Policy Makers in the Government of India from CERT-In, NTRO, Office of NSA and leading Suppliers across both Oil & Gas industry and Security Providers were handpicked based on their expertise and knowledge in the sector. In depth interview was conducted by using the Interview Protocol attached in the Appendix.

Size of the given sample of the qualitative analysis is not pre-determined, sampling is continued till we attain the Theoretical Inundation or till such time no new data emerges. The researcher conducted 8 in depth interviews till no new data began to emerge. The interviews then were recorded and served as the inputs for interpretation. Interpretation of Data in Qualitative Analysis was done using Ritchie and Spencer's Framework Analysis.

The profile of the respondents are as follows:-

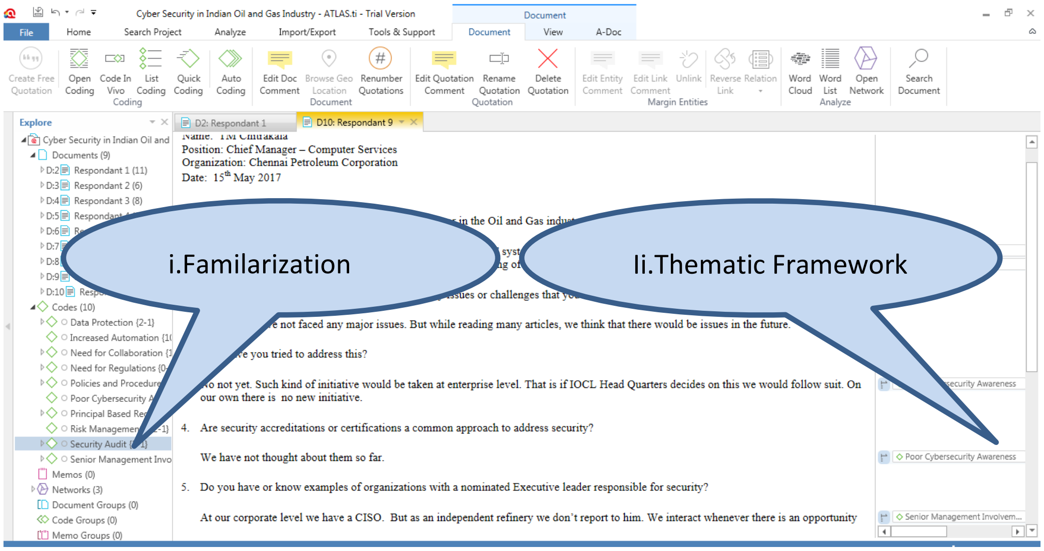
1. Senior Manager, Information Systems (IS), IOCL
2. Executive Director (Retired), IOCL
3. Deputy General Manager, (IS) ONGC
4. General Manager Information Systems (IS), HPCL
5. Senior Manager (IS), BPCL
6. Consultant, IBM, Ex IOCL, Ex GAIL, Ex PWC
7. Associate Dean – PG (Professor – Dept. of Oil & Gas), University of Petroleum and Energy (UPES), Dehradun
8. Dean and Professor, Department Petroleum Management, School of Petroleum Management, Pundit Dindayal Petroleum University (PDPU)

5.2.1 DATA INTERPRETATION

Ritchie & Spencer's Framework Analysis has 5 components namely: Familiarization, Identifying a Thematic Framework, creating a catalogue, Chart drawing, Mapping & Elucidation, as detailed out in previous chapters. The transcripts were revised a number of times to gather the key themes and identify patterns. Indexing which is the third step in the framework analysis was done in this research using Atlas TI and is elaborated in the succeeding section.

5.2.2 THEMATIC FRAMEWORK

A number of common themes appeared from this in-depth interviews. These include reference to the new Hydrocarbon Exploration and Licensing Policy (HELP), as a stimulus for investment in the Oil & Gas industry, the investment in IT driving increased automation in Oil & Gas industry, poor security awareness, and lack of executive ownership of cybersecurity, little or no information sharing and collaboration within the industry, need for data protection. The familiarization and identifying thematic framework is shown in Figure 5.1 below.



Name: TM Chitrakala
Position: Chief Manager – Computer Services
Organization: Chennai Petroleum Corporation
Date: 15th May 2017

in the Oil and Gas indu

syst
ng of

ssues or challenges that yo

e not faced any major issues. But while reading many articles, we think that there would be issues in the future.

ve you tried to address this?

o not yet. Such kind of initiative would be taken at enterprise level. That is if IOCL Head Quarters decides on this we would follow suit. On our own there is no new initiative.

4. Are security accreditations or certifications a common approach to address security?

We have not thought about them so far.

5. Do you have or know examples of organizations with a nominated Executive leader responsible for security?

At our corporate level we have a CISO. But as an independent refinery we don't report to him. We interact whenever there is an opportunity

Figure 5-1 Classification of Multi-variate Techniques

5.2.3 INDEXING

Coding and Indexing is the approach to labelling data into adaptable portions for subsequent recovery and exploration. Atlas TI enabled us to break the pain of coding by automating a number of intermediate tasks. The sample screen shot of indexing using Atlas TI is caught in Figure 5.2 given below. The codes that were identified are mapped back or "indexed" to the themes that emerged from the in-depth interview.

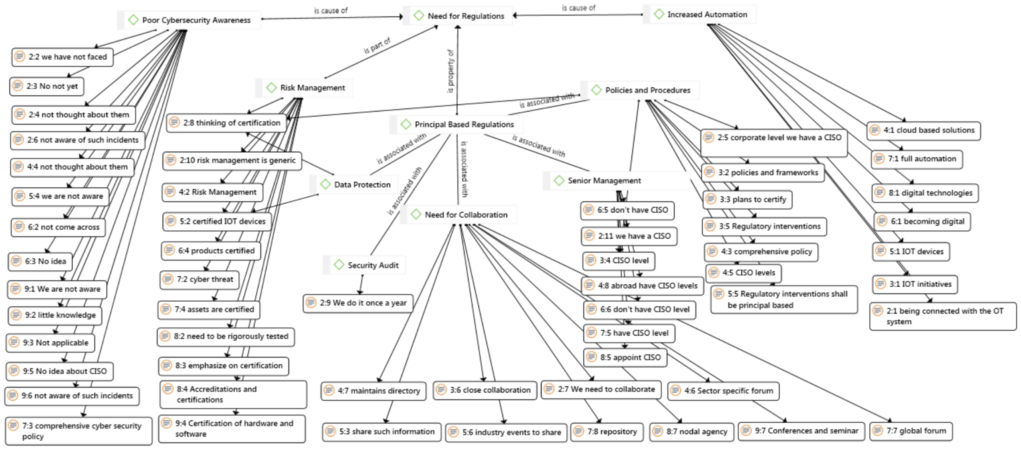


Figure 5-2 Indexing, Charring and Mapping using Atlas TI

5.2.4 Charting & Mapping

The relationship between the themes were identified and mapped that became the input for interpretation stage.

5.2.5 Interpretation

Interpretation of in-depth interviews is not just reporting or transcribing of the various interviews. It includes brining up of the expert opinion assembled in the sessions with the existing knowledge or theory to elicit a clear conclusion. The interpretation would need to consider the relevant background of the Indian Oil & Gas industry and related constructs. The next section offers a relevant environment of the present Oil & Gas industry, in India, relevant to this research.

5.2.6 Background

Among the other core industries in India, the decision making element in the economy is found to be the petroleum sector. To fill the steadily on going increase in the gap between India's petroleum supply and demand, a New Exploration Licensing Policy (NELP), was projected in 1997-98. (MOPNG, n.d.). India's growth in economy is directly proportional to energy needs and hence the Oil and Gas sector is likely to grow more. This would encourage reasonable investment in the sector. Numerous policies were executed by the Indian Government to satisfy growing demand. Now all Government allows mostly 100% Foreign Direct Investment (FDI) across the Oil and Gas value chain.

Among the non-OECD petroleum globally, the consumption growth of the India is expected to be one of the largest providers. The natural gas & petroleum sector attracted FDI nearly US$ 6.86 billion amid 2000 to 2017, according to data discharged by Department of Industrial Policy and Promotion. (Moumita Samantha, 2018).

The Government of India is also coming out with new plan to integrate state oil companies to make them as integrated oil majors, so that they could compete globally. This would also help them develop the interaction between various state bodies for attaining efficiency, competency and affordability and create more value for all shareholders. (Economic Times, 2016).

The Government of India wants to bring in more investments into these fields. So they have come out with a plan to disclose a new policy for both renewing & extending the company lease of nearly 28 Oil & Gas blocks in the country. (Economic Times, 2017).

India’s demand for oil is anticipated to increase at an approximate rate of CAGR 3.6 % to 459 MTOE in future, while need for energy would multiply several times by 2039, as economy would grow by more than 5 times its current size, as per the Petroleum & Natural gas ministry. (Economic Times, 2015).

Looking into IOT impact in all business, Indian enterprises seem to be in the nascent stage according to Gartner, Inc. (Gartner, 2015). However, although IoT is gaining reputation, safety and security alarms and the absence of relevant business cases may hamper the adoption of the technology in the immediate term, but the adoption may improve in future in slow pace. According to Gartner, the adoption of IoT technology India is presently restricted to a few verticals including energy, utilities as well as oil & gas. (Gartner, 2015). In India, only very few organizations in the oil and gas industry, have commenced pilot projects for IoT, in the areas of pipeline networks management using IOT devices. (Gartner, 2015).

As reported by Ganesh Ramamoorthy, VP, Gartner, the Indian companies have attempted reasonable business cases for IoT solutions and the government has taken swift steps for embracing the IoT technology and introducing new business opening for solution providers dealing with the IoT based solutions. (Ganesh Ramamoorthy, Gartner, 2015). The initiatives sponsored by the government would be the crucial handlers for the IoT adoption in our country for the next 5 years. Sectors implementing the IoT projects would see a surge in data centers and also in the storage cost since the

IoT projects would generate terabytes of big data, which needs to be seamlessly stored, appropriately processed and effectively analyzed. (Gartner, 2015).

As per Aman Munglani, research director of Gartner, the impact of the IoT would be significant as there would be enormous amount of data that would be stored and maintained, which may perhaps affect how data centers are managed. (Gartner, 2015) Managers involved in IoT product may have to handle the challenge of scalability as well cost-effective value. (Gartner, 2015).

The increased IT adoption, has delivered a number of benefits for the Indian Oil & Gas industry. There was universal recognition amongst the respondents on recent investments and policies in the industry as the single biggest stimulus to IT investment in the Indian Oil & Gas industry. There are a number of IT lead initiatives that are undertaken and examples of how IT adoption has improved significantly in the Smart Fuel Station, Integration of IT/OT systems. The increased adoption of IT was noted as a definite positive across the spectrum of respondents.

They pointed out that cybersecurity seldom features in discussions on IT programs, and this was the second point where there was unanimity of opinion.

The respondents brought out that barring a few establishments, the role of a CISO or a similar role was not well established in the Indian Oil & Gas industry. The role of security executive leadership was assumed to be part of the IT team or subsumed with the CIO organization. A common theme across the respondents was the minimal awareness both at the executive level and other members of the industry regarding the cybersecurity controls.

5.3 ANSWER TO THE RESEARCH QUESTION RQ1

The summary of the outcome of the qualitative analysis to identify the challenges in the Indian Oil & Gas industry is portayed in the below Figure 5.3.

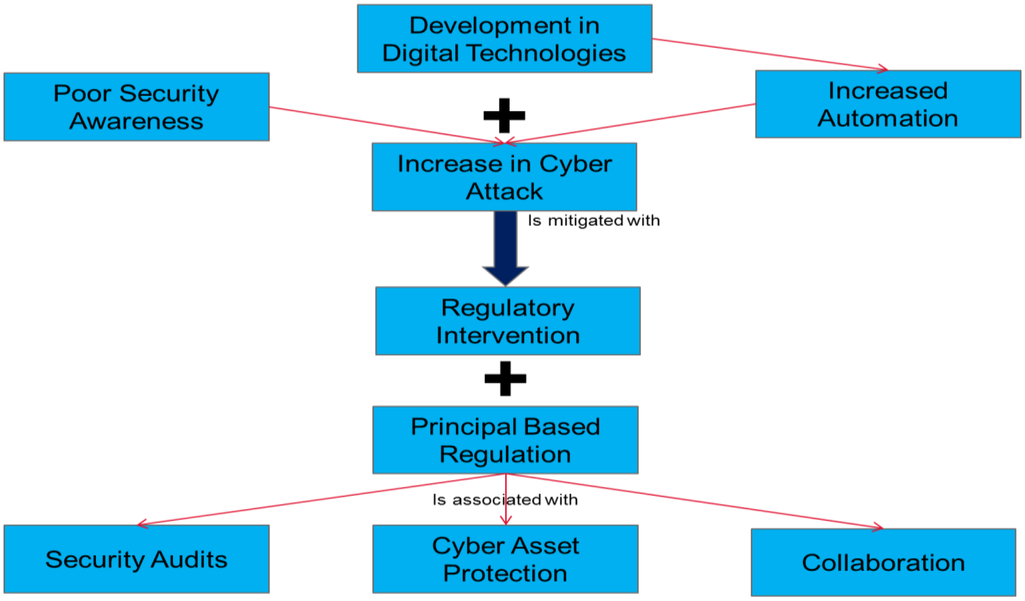


Figure 5-3 Summary of the Qualitative Analysis

The increased IT adoption, driven by the new exploration program has delivered number of benefits across all the Oil & Gas companies. However, very little appreciation of the risks or exposure to cybersecurity threats which comes along with the increased adoption of IT both among the executives and the non-executive employees of the Oil & Gas industry. A majority of the establishments don't have designated CxO level executive responsible for cybersecurity and the security function is usually included within the IT organization. Given the diversity and the financial status of the players in the Oil & Gas industry, a principal based regulatory intervention emerged as a preferred choice to enrich cybersecurity in Oil & Gas industry. A principal based regulatory intervention unlike a rule based mandate would do away with detailed technical controls to be included in the mandate. Data protection, critical cyber asset protection, risk based audits and information sharing and collaboration were the domains that were identified as components in the mandate.

This answers our very first research or investigation question RQ1.

5.4 Quantitative Data Analysis – Objective 2

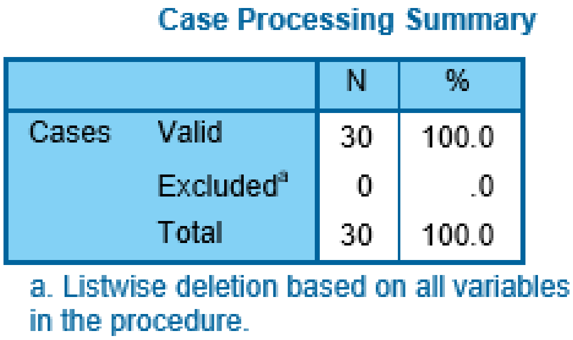
The starting point of the quantitative data analysis was the output of the qualitative analysis, the original set of 24 variables that emerged from the literature review was narrowed down to 21 variables. The variables were administered on 5 point Likert-type scale to the respondents.

5.4.1 Test of Reliability – Cronbach's Alpha

The questionnaire was first piloted in person to respondents and then corrected to remove ambiguity. The response of the initial set of 30 respondents was assessed for reliability and validity using SPSS.

The internal reliability was measured using Cronbach's alpha. The Cronbach's alpha score of **0.938** as shown in Table 5.1 is more than the threshold of 0.7 and is deemed as an acceptable score. (Schutte, Toppinnen, Kalimo, & Schaufeli, 2000) This proves that the instrument meets the reliability requirement for further process.

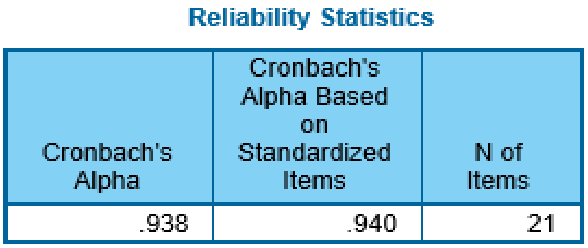
Table 5-1 Cronbach's Alpha Score Based on First 30 Respondents



Case Processing Summary

		N	%
Cases	Valid	30	100.0
	Excluded[a]	0	.0
	Total	30	100.0

a. Listwise deletion based on all variables in the procedure.

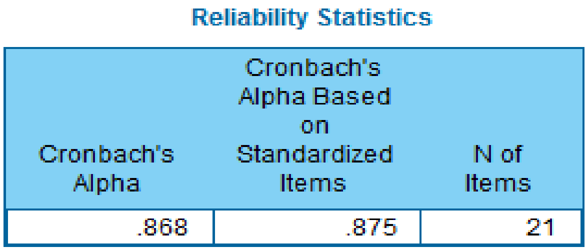


Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.938	.940	21

The Cronbach’s alpha test was repeated once the entire data collection (for 305 respondents) was completed before the factor analysis. This showed a new Cronbach’s alpha score of **0.868** as shown in Table 5-2 below.

Table 5-2 Cronbach’s Alpha Score with All the Respondents



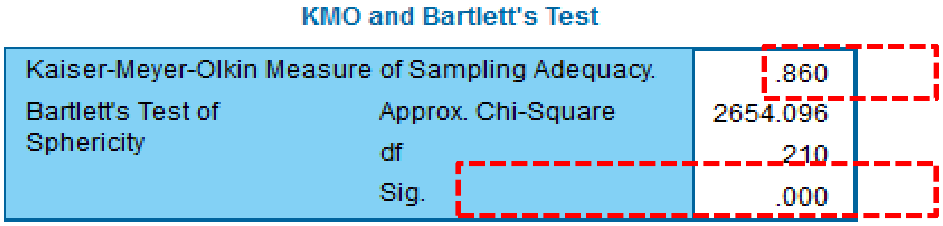
Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.868	.875	21

5.4.2 KMO & Bartlett’s Test

The sampling adequacy is measure by the Kaiser-Meyer-Olkin (KMO) index and Sphericity test of Bartlett checks the hypothesis that the variables form an identity matrix with no co-relation between them. The KMO score of **.860** as shown in Table 5.3 is deemed as meritorious and confirms the sampling adequacy of the research. (Dziuban & Shirkey, 1974). Table 5.4 gives an overview on interpreting the KMO score. Sphericity test of Bartlett also checks the hypothesis that the variable are independent. The researcher was able to reject the hypothesis as the significance is .000. It is now confirmed that the data set can proceed to factor analysis as it is ready.

Table 5-3 KMO and Bartlett's Test



KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.860
Bartlett's Test of Sphericity	Approx. Chi-Square	2654.096
	df	210
	Sig.	.000

Table 5-4 Interpreting the KMO Score

Interpreting KMO Score	
0.9 +	**Marvelous**
0.8 – 0.9	**Meritorious**
0.7 – 0.8	**Middling**
0.6 – 0.7	**Mediocre**
0.5 – 0.6	**Miserable**
0.4 – 0.5	**Unacceptable**

5.5 Exploratory Factor Analysis (EFA) Result

EFA is statistical technique that deals with multiple variables. It focusses in identifying structure and factor that explains the inter-connection amid a set of variables observed. It works on a technique called data reduction technique in which we get small factors out of these observed variables by abridging them. EFA transforms the correlations in the set from the observed variable into a smaller number of basic factors. This still retains the vital information about the linear interrelationships found in the original variables.

There are 3 decision points in factor analysis. The decision points are listed below and discussed as follows. (Costello & Osborne, 2005).

5.5.1 EXTRACTION - COMPONENT VS. FACTOR EXTRACTION

Though there are a number of different approaches to Extraction, still there are challenges faced by the researchers in narrowing down to the appropriate method. They point out the lack of literature on the merits and demerits of the various options and a more basic disagreement on the very basics of the extraction methods. Principal Component Analysis and Common Factor Analysis are by far the two most popular choices amongst the researchers. (Costello & Osborne, 2005).

All the variables are taken for consideration in PCA and further pursues a linear blend of variables. Here the greatest variance is extracted and this process is repeated till all the factors are extracted. It results in an orthogonal array of uncorrelated factors.

Now when the Common Factor Analysis is taken, it is found that it takes only the common variance. It seeks to identify the least number of factors that can account for the common variance or correlation of set variables.

There are multiple schools of thought that favor one extraction method over the other with some statistical theorists arguing that component analysis is not a true method of factor analysis, while the researchers arguing for component analysis and suggest that there is no difference between the two. This research uses Principal Component & Analysis for Extraction.

5.5.2 NUMBER OF FACTORS TO RETAIN

The next decision point after extraction is to determine on the number of correct factors to keep. The “cleanest” factor structure would imply that all item loadings above 0.30, there no or very few item cross-loading and no factors with lesser than 3 items. (Costello & Osborne, 2005). There are a variety of approaches to arrive at the number of factor that has the best fit to the data

- Retain all factors with Eigenvalue of 1 or more.
- When Examination of the scree plot of Eigenvalues for the break point in data in which the curve flattens out, it is observed that the number of data points above the “break” is the number of eligible factors to retain.

This research uses the first approach of retaining all factors with Eigenvalues of 1 or more to arrive at the number of factors for retention

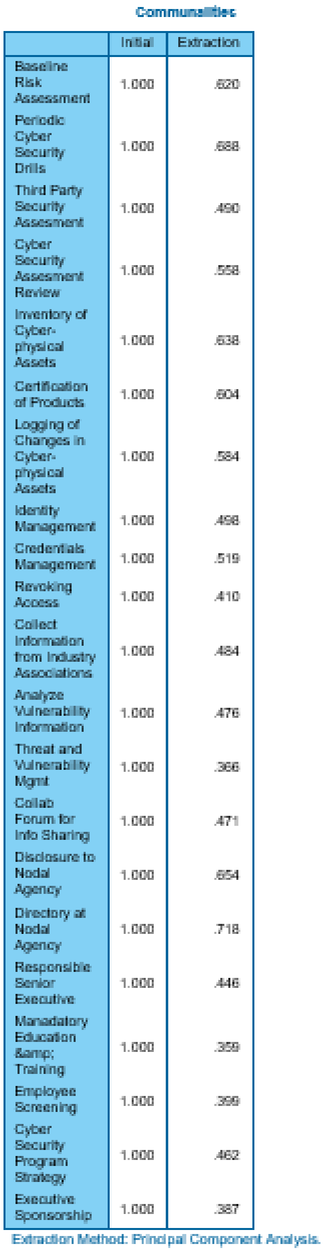
5.5.3 ROTATION

Rotation facilitates interpretation by differentiating the data. (Gaskin, Exploratory Factor Analysis, 2012). Orthogonal and Oblique are the two alternative approach to rotation. Orthogonal rotations produces factor which is uncorrelated while oblique rotation methods permit the produced factors to compare and relate to each other. Varimax, Quartimax and Equimax are types of orthogonal rotations, while Direct Oblim and Promax are Oblique rotations. This research uses the Varimax for Rotation.

5.6 COMMUNALITIES

Communality is a measure to which an item connects with rest of the other items. Higher the communality, better the correlation. When the communalities for a specific variable is found to be low (< 0.4), it would imply that the variable would struggle to load significantly on any factor. (Gaskin, Exploratory Factor Analysis, 2012). The Table 8-5 below shows the communality for the research data. There are no Low values to indicate candidate variables for removal and all the variables are carried for factory extraction.

Table 5-5 Communalities



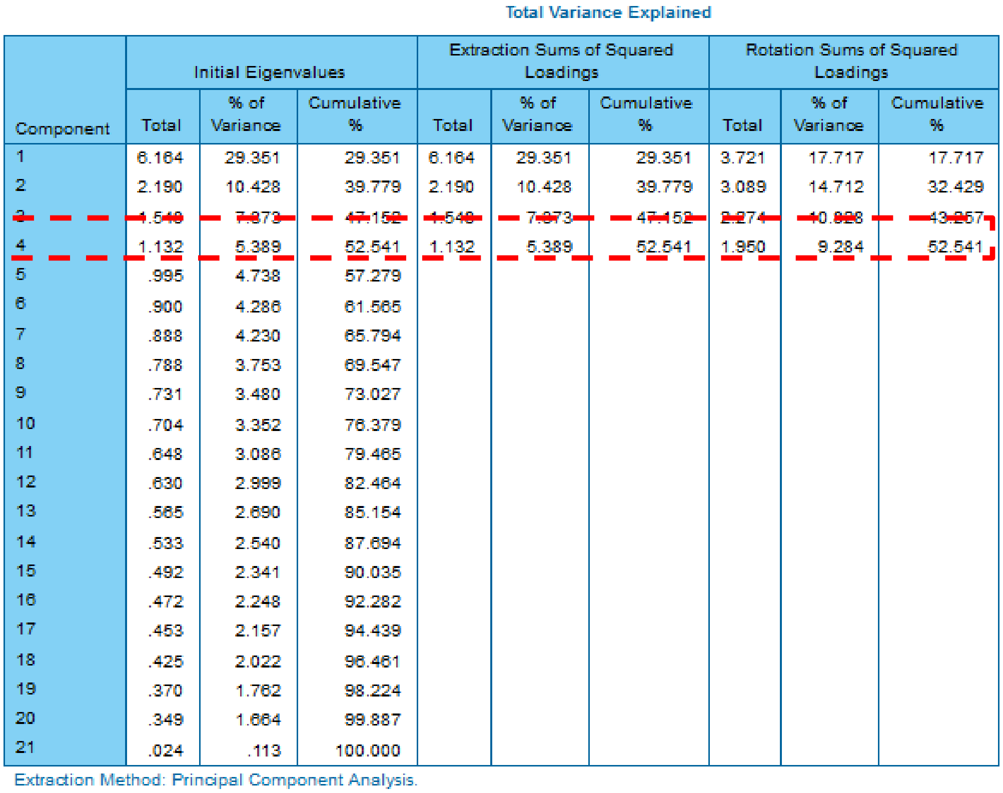
Communalities

	Initial	Extraction
Baseline Risk Assessment	1.000	.620
Periodic Cyber Security Drills	1.000	.688
Third Party Security Assesment	1.000	.490
Cyber Security Assesment Review	1.000	.558
Inventory of Cyber-physical Assets	1.000	.638
Certification of Products	1.000	.604
Logging of Changes in Cyber-physical Assets	1.000	.584
Identity Management	1.000	.498
Credentials Management	1.000	.519
Revoking Access	1.000	.410
Collect Information from Industry Associations	1.000	.484
Analyze Vulnerability Information	1.000	.476
Threat and Vulnerability Mgmt	1.000	.366
Collab Forum for Info Sharing	1.000	.471
Disclosure to Nodal Agency	1.000	.654
Directory at Nodal Agency	1.000	.718
Responsible Senior Executive	1.000	.446
Manadatory Education &amp; Training	1.000	.359
Employee Screening	1.000	.399
Cyber Security Program Strategy	1.000	.462
Executive Sponsorship	1.000	.387

Extraction Method: Principal Component Analysis.

The Table 5.6 on total variances below gives the amount of variance explained by each component where the cumulative sum adds up to 100%. The first four factors where the Eigenvalues is of 1 or more represent 52.5 % of the total variance in the 21 variables.

Table 5-6 Factor Analysis – Four Factors explain 51.6% of the Variance



Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	6.164	29.351	29.351	6.164	29.351	29.351	3.721	17.717	17.717
2	2.190	10.428	39.779	2.190	10.428	39.779	3.089	14.712	32.429
3	1.549	7.373	47.152	1.549	7.373	47.152	2.274	10.828	43.257
4	1.132	5.389	52.541	1.132	5.389	52.541	1.950	9.284	52.541
5	.995	4.738	57.279						
6	.900	4.286	61.565						
7	.888	4.230	65.794						
8	.788	3.753	69.547						
9	.731	3.480	73.027						
10	.704	3.352	76.379						
11	.648	3.086	79.465						
12	.630	2.999	82.464						
13	.565	2.690	85.154						
14	.533	2.540	87.694						
15	.492	2.341	90.035						
16	.472	2.248	92.282						
17	.453	2.157	94.439						
18	.425	2.022	96.461						
19	.370	1.762	98.224						
20	.349	1.664	99.887						
21	.024	.113	100.000						

Extraction Method: Principal Component Analysis.

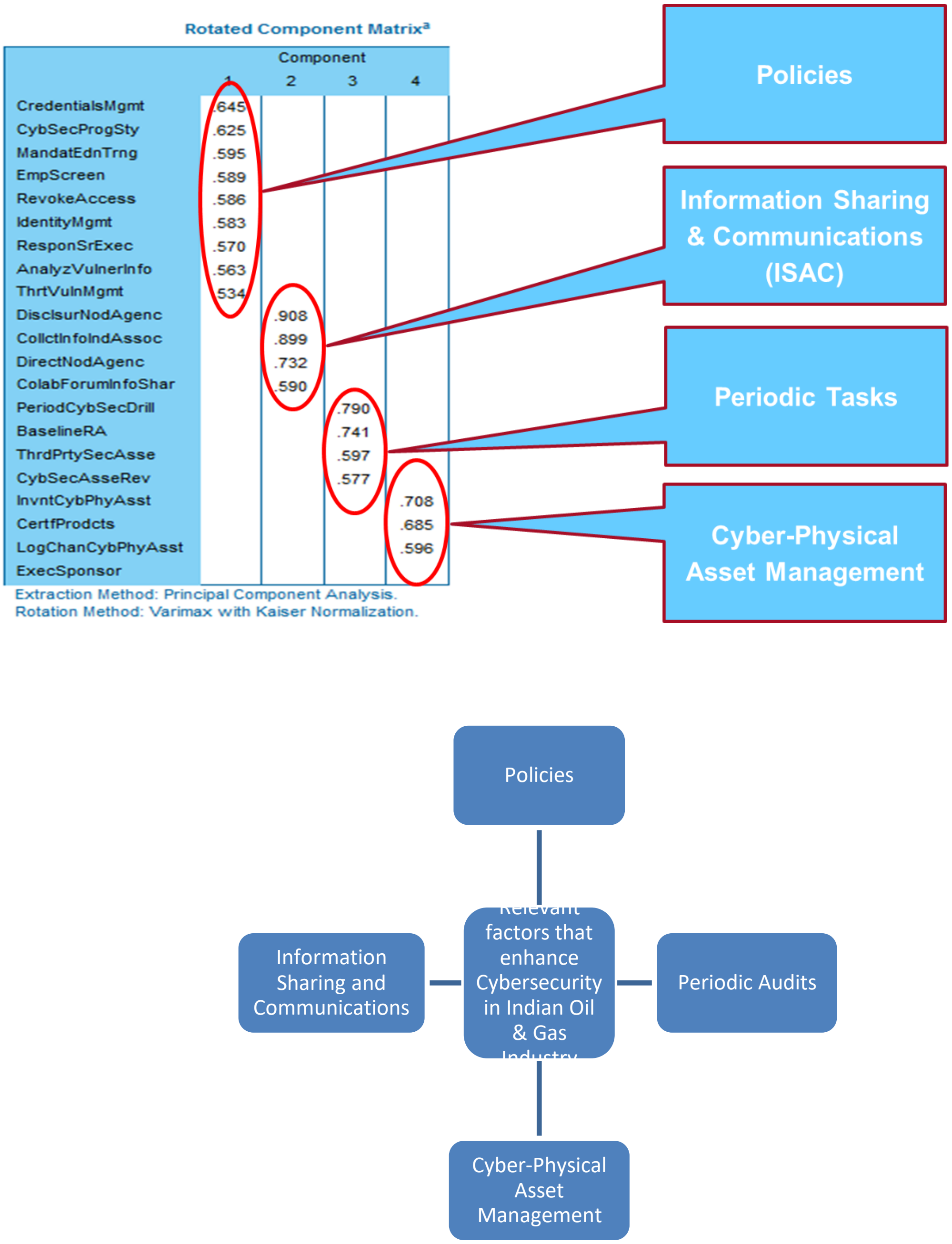
5.7 Rotated Component Matrix

The rotated component in Table 5.7 shows the 21 variables loading onto 4 factors. This is in line with the co-variances explained Table 5.6 above, meeting the requirements of "clean" factor loading requirements of Costello & Osborne considered in the preceding section of the chapter.

5.8 Answer to the first part of RQ2

The factors that emerged from the Exploratory Factor Analysis answers the first part of the RQ2. The four factors that deepen cybersecurity in the Indian Oil & Gas industry are shown in Table 5.7 below.

Table 5-7 Rotated Component Matrix



Rotated Component Matrix[a]

	Component			
	1	2	3	4
CredentialsMgmt	.645			
CybSecProgSty	.625			
MandatEdnTrng	.595			
EmpScreen	.589			
RevokeAccess	.586			
IdentityMgmt	.583			
ResponSrExec	.570			
AnalyzVulnerInfo	.563			
ThrtVulnMgmt	.534			
DisclsurNodAgenc		.908		
CollctInfoIndAssoc		.899		
DirectNodAgenc		.732		
ColabForumInfoShar		.590		
PeriodCybSecDrill			.790	
BaselineRA			.741	
ThrdPrtySecAsse			.597	
CybSecAsseRev			.577	
InvntCybPhyAsst				.708
CertfProdcts				.685
LogChanCybPhyAsst				.596
ExecSponsor				

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

Policies
Information Sharing & Communications (ISAC)
Periodic Tasks
Cyber-Physical Asset Management
Policies
Information Sharing and Communications
Relevant factors that enhance Cybersecurity in Indian Oil & Gas Industry
Periodic Audits
Cyber-Physical Asset Management

Figure 5-4 Factors to Enhance Cybersecurity in Indian O&G Industry

5.9 CONFIRMATORY FACTOR ANALYSIS (CFA)

The path models or path diagram are the foundation building blocks for both Structural Equation Modelling (SEM) and Confirmatory Factor Analysis (CFA). The Path diagrams are like flowcharts that depict the interconnection of the variables and their causal flow (Steiger, n.d.). The path flow diagrams follow a standard convention where all the latent are depicted in an ellipse, all the indicators or variables are shown in rectangular boxes, error terms or residual terms are found in a circle. The arrows depict the causal relation.

Schreiber et al in their review paper provide a structure and approach to reporting on CFA / SEM research. (Schreiber et al., 2006). They identify both the technical and non-technical evaluative issues that needs to be included while reporting CFA.

They identify six nontechnical issues in evaluating a CFA article that is identified below:

- Research question(s) that dictate the use of CFA
- Discuss the rationale for CFA or SEM
- Provide the measurement model's conceptual and / or structural framework (or the theoretical grounding for the model)
- Appropriate tables and figures
- A graphic exhibit of the hypothesized or final CFA model and
- Inference from the findings

The survey also highlights the technical issues to include pre-analysis and post analysis. The pre-analysis technical issues are:

- Sample size
- Software Used

On the post analysis however, there is no single set of metrics that is universally accepted. Schreiber et al.'s survey identifies a number of different threshold metrics

(Schreiber et al., 2006) to evaluate “goodness of fit”, including Hu and Bentler’s (Hu & Bentler, 1999) thresholds that is references in this research. They go on to point out that when a model has been changed and analyzed again, evidence that the modified model is statistically superior to the original model should be included and with the theoretical reasons for the modifications.

5.9.1 RESEARCH QUESTION THAT DICTATE THE USE OF A CFA

The research question for this research was arrived at, from the research gap identified in the literature review in the previous chapters on Literature Design. The **RQ** is “What are the relevant factors that enhance the cybersecurity and their significance in the Indian Oil & Gas industry” The factors identified using EFA and CFA is proposed to establish their significance

5.9.2 THE RATIONAL FOR THE CFA

The rationale and approach to CFA has been detailed out in the previous chapter on Research Design. Next step is the CFA after EFA, the Exploratory Factor Analysis to determine the given factor structure. The EF Analysis elaborates on the relationship between the variables and group, based on inter-variable correspondences, while the CFA confirms the given factor structure extracted in the EFA (Gaskin, Confirmatory Factor Analysis, 2012).

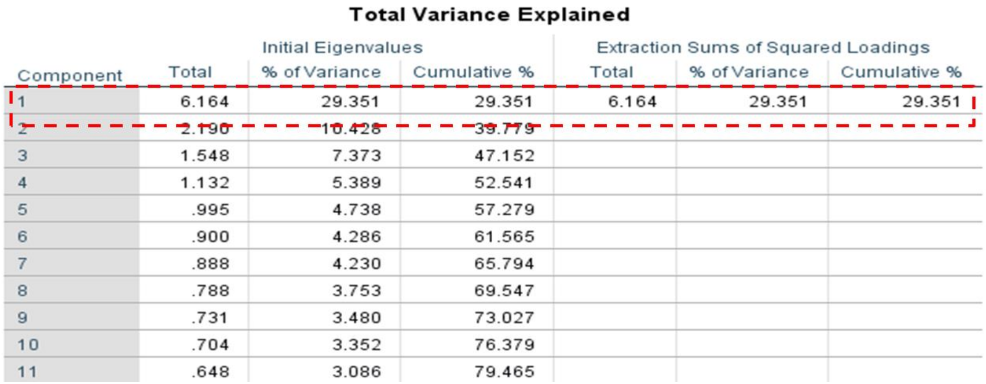
5.10 EVALUATING COMMON METHOD BIAS

A dataset is said to exhibit a Common method bias if there is one factor that explains a majority of the variance. Harman’s single factor test is used for evaluation for the common method bias. This is done by constraining the number of factors gotten in the EFA to just one, rather than extracting the factors via Eigenvalues. Common Method Bias is said to exist, if the single factor explains a majority of the variance issue (Gaskin, Confirmatory Factor Analysis, 2012).

5.10.1 HARMAN'S SINGLE FACTOR TEST

The result of the Harman's single factor test shows that cumulative loading accounts for only 29.4% of the variance as shown in Table 5.8 below. Common method bias is said to exist if one single factor explains 50% or more of the total variance. This confirms that that there is NO common method bias in the data.

Table 5-8 Total Variance Explained



Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	6.164	29.351	29.351	6.164	29.351	29.351
2	2.190	10.428	39.779			
3	1.548	7.373	47.152			
4	1.132	5.389	52.541			
5	.995	4.738	57.279			
6	.900	4.286	61.565			
7	.888	4.230	65.794			
8	.788	3.753	69.547			
9	.731	3.480	73.027			
10	.704	3.352	76.379			
11	.648	3.086	79.465			

5.11 ANSWER TO RESEARCH QUESTION – RQ2

The original EFA identified five factors that enhance cybersecurity in the Indian Oil & Gas industry. The subsequent path model analysis and measures of the model fit using Confirmatory Factor Analysis narrowed down the factors to four that are significant.

5.12 CONCLUDING REMARKS

The Data analysis section focused on executing the blue-print that is laid out as part of the research design. The challenges in the Indian Oil & Gas industry or the research question 1 (RQ1) was answered using the qualitative research. The RQ2 which was to identify the factors that enhance cybersecurity and their significance was answered by the quantitative analysis.

The qualitative analysis established the drivers and need for cybersecurity in the Indian Oil & Gas industry and the need for regulatory intervention. The detailed interviews helped to bring down the variables to a smaller set of 21 which were very much relevant to the Indian scenario. These variables were the input for the quantitative analysis to answer the RQ2. The reliability and validity was established. The exploratory factor analysis helped identify the initial set of four factors - **Information Sharing & Collaboration, Polices, Cyber-Physical Asset Management and Periodic Audits** that improve cybersecurity in the Indian Oil & Gas industry. The subsequent confirmatory factor analysis established these as significant factors in the Indian context.

6 CONCLUSION AND REMARKS

6.1 OVERVIEW

This section reviews the recommendations for enhancing cybersecurity in the Indian Oil and Gas industry. The constituents developing a mandate for enhancing the cybersecurity for the Indian Oil and Gas are (i) Information Sharing and Collaboration, (ii) Policies, (iii) Cyber-Physical Asset Management, (iv) Periodic Audits. This chapter also emohasizes the research contributions, research limitations and future scope for further research in the allied topics.

6.2 CONCLUSION

The objective of the research was to identify the constituents of the cybersecurity mandate for the Indian Oil and Gas industry. The framework analysis of the in-depth interview with experts in the Oil and Gas industry identified the key challenges in the Indian Oil and Gas industry and helped identify the variables that are relevant to the Indian context. After a detailed survey with more than 300 respondents, the variables are under 4 major factors. CFA technique was also used to verify this model. Once again the research outcome has been discussed with the 8 industry experts, who were in agreement with the research outcome.

6.3 RECOMMENDATIONS

The diversity of the Indian Oil and Gas industry and the financial constraints plaguing the sector, an intervention in the form of a principle based security mandate by the regulatory authority is regarded as the preferred vehicle to enhance cybersecurity in the Indian Oil and Gas industry. In present day’s networked world, critical infrastructure protection is national priority. The Oil and Gas industry bears the brunt of cyber threats globally with nearly half the cyber-attacks on critical infrastructure targeting the energy sector. India’s Oil and Gas industry is stressed with a number of issues, but would need to make cybersecurity a priority and would need to respond quickly to protect its safety and ensure continued economic progress and prosperity. The recommendations coming out of the research are articulated below

i. Mandatory Oil and Gas Sector-specific Cybersecurity Guidelines

The Ministry of Petroleum and Natural Gas should formulate mandatory Oil and Gas sector-specific cybersecurity guidelines. To start with, the mandatory guidelines can be principle focused i.e. at a high level rather than specific guidelines. But going forward, it should slowly start addressing the different sub-businesses of the streams, since the impacts due to cybersecurity incident vary for different transactions of the petroleum value chain. Hence specific guidelines for Exploration and Production in Upstream segment, Energy Trading and Risk Management (ETRM), Pipelines, Shipping in Midstream segment and Refining and Retail Marketing in Downstream segment can be thought of.

ii. Responsible Senior Person as Cybersecurity Custodian

The role of information technology in oil and gas industry has undergone a sea-change in the past two decades. Also with the arrival of the Internet of Things (IoT) technology and the concepts of digital transformation in the coming days, the role of IT would be significant. Hence, it is vital for the Indian oil and gas industry to have the senior executive roles such as Chief Information Security Officer (CISO). In fact, if the company is has an integrated operations i.e. having presence in multiple chains, they can think of having individual CISOs for every segment of the value chain. The individual CISOs can report to a Group CISO, who may be treated on par with the Directors. This way the accountability and responsibility towards cybersecurity can be enhanced.

iii. Workforce Management

When the impact due to cybersecurity incident would be going higher and higher in the coming days, there is need for a security awareness culture across the organization at all levels. Though the detailed and periodic training is mandatory for the IT group, the other groups should also be exposed to the basic training modules on cybersecurity. This essential as each one of them handle vital data and information, whose breach can make a huge impact on the business. The organization should also bring in compulsory background screening and vetting of the employees, before they are on-boarded.

iv. Critical Cyber-Physical Asset Protection

Security certifications are required for critical cyber-physical assets. Organizations should identify, maintain a baseline their critical cyber-physical assets. These assets should be subject to period security audits. This step would become essential as organizations would start encouraging its employees to adopt the concept of "Bring Your Own Devices" (BYOD). The role of IoT devices in the industry would make the certification and periodical assessment of the cyber-physical assets a mandatory one.

v. Information Sharing and Collaboration

In the USA, ONG-ISAC is a central pool of cyber threat information for the O&G industry. It takes care of different segments of the Oil and Gas value chain from cyber threats by timely sharing of the cyber intelligence. This body offers a platform for members to share cyber intelligence information between members. In Europe, there exists an initiative called, "The Thematic Network on Critical Energy Infrastructure Protection" (TNCEIP). The initiative of the European Commission is to bring together the European owners and operators in the electricity, gas and oil sectors. Members of this program periodically exchange information related to cyber incidents.

In India, a similar organization specifically catering to the cybersecurity needs of the Oil and Gas industry is yet to evolve. The government should take necessary measures to set up a critical incident response team and define the process to react to a cyber-emergency. The ministry should facilitate the setup of a forum for the players in the Oil and Gas industry and promote information sharing and collaboration including disclosure of cybersecurity incidents. Information Sharing and Communication policy makers need to focus on

- Setting up a nodal agency maintaining current directory of industry wide cybersecurity emergency response contacts.
- A mechanism for the disclosure of breaches and security incidents in Oil and Gas industry to the nodal agency.
- Collecting useful information from reliable sources like Industry Associations, CERT etc.
- Work with industry specific collaboration forum to share security knowledge, incidents and best practices.

vi. Security Audits

Oil and Gas industry should start conducting self-assessments for evaluating their cybersecurity posture, which shall be followed by periodic third party security audits. This can be similar to the Cybersecurity Capability Maturity Model (C2M2) framework that is being used in the Oil and Gas industry in the United States. Regulatory body should facilitate Industry wide security drills to prepare the organizations to handle a real life cybersecurity incident. In the Oil and Gas industry, the IT implementation and the plant automation are there for so long. With the arrival of the IoT devices, the industry should quickly go towards larger adoption of IT and digital transformation. In this context, security assessments and audits would enhance the cybersecurity to a great extent.

vii. Collaboration with Academic Institutions

There are few reputed academic institutions like University of Petroleum and Energy Studies (UPES), Dehradun, Pundit Dindayal Petroleum University (PDPU), Gandhinagar, Rajiv Gandhi Institute of Petroleum Technology, Rae Bareli offering multitude of courses in the Oil and Gas segment. Since the industry cannot afford to have too many people in their Cybersecurity team, the industry can collaborate with the above institutions in the following areas:-

- Knowledge sharing
- Reverse knowledge sharing
- Tri-party arrangements
- Policy formulation & Updating

6.4 RESEARCH CONTRIBUTION AND THEORETICAL CONSTRUCT

In this research, the researcher has identified the components for the cybersecurity mandate in the Indian Oil and Gas industry. The research helped zeroed in four major elements that would contribute to augment the security aspects in the Indian Oil and Gas industry. The 4 factors are:-

1. Identity & Access Mgmt.
2. Risk Mgmt.
3. Asset, Change and Configuration Mgmt.
4. Information Sharing and Collaboration

Laudon and Trever suggested a 4-layer cybersecurity model for the e-Commerce industry. Data Protection, Technology, Organization Policies and Procedures with Laws & Industry standards forming the model. All the 4 layers are relevant to the Oil and Gas industry as well. However the oil and gas industry brings with it industry-specific Information Sharing and Collaboration, which does not have relevance in the e-commerce industry. The contribution to theory from this research is the extension of the Laudon and Trever’s 4 layer e-commerce security model by including the “Industry-specific Information Sharing and Collaboration” regarding the Oil and Gas industry’s cybersecurity.

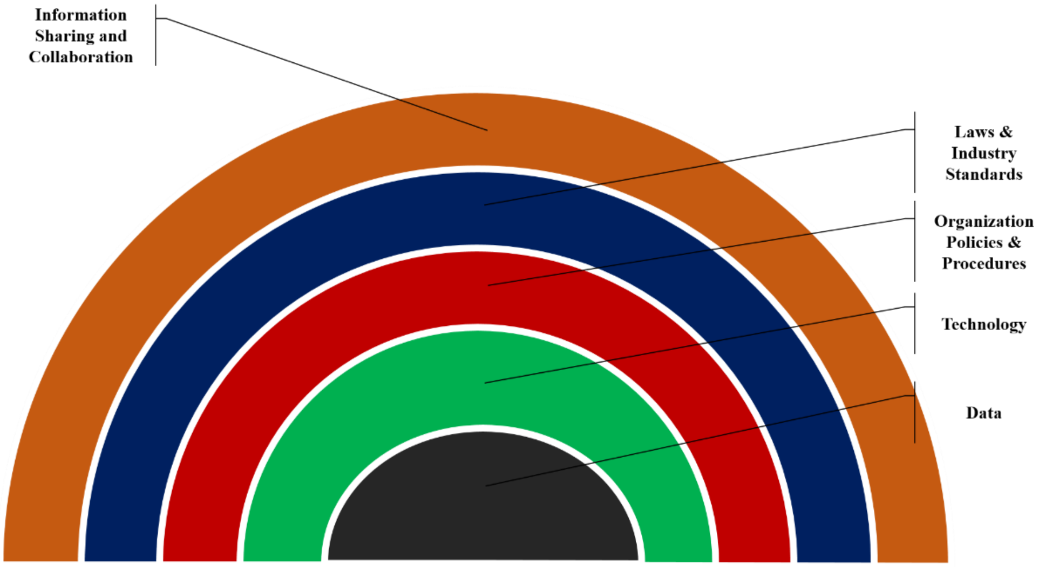

Information Sharing and Collaboration
Laws & Industry Standards
Organization Policies & Procedures
Technology
Data

Figure 6-1 Extn. of Laudon & Trever's Cybersecurity Model for O&G

6.5 Limitations of the Study

The research study was concentrated on developing the cybersecurity mandate for the Indian Oil and Gas industry. At the end of the study, four factors were identified that would enhance the cybersecurity position of the Indian Oil and Gas industry. However the study has few limitations.

1. The scope of the study was restricted to India. Because the choice of the variables, the sample size and extent were all limited to India, the model adopted in this study of statistical analysis to identify factors and establishing their significance has widespread application, cannot be generalized to other geographies or nations.

2. In India, cybersecurity in the Oil and Gas industry is still in the burgeoning stage with modest published literature. The results from the in-depth interviews of the respondents or the survey would be built on their current perceptions. These could change with their increased exposure and experience

in the sector, especially after digital transformation happening in the industry. This may affect the outcome.

3. Within various departments of Government of India, there is minimal publications on the cybersecurity policy and guidelines. The research has primarily used data from public domain for understanding and interpreting the cybersecurity polices of the Government of India.

4. In this research, the researcher has used Principal Component Analysis for Exploratory Factor Analysis and Orthogonal Rotation for extraction of factors. Some other selection of statistical techniques may impact the original set of factors.

5. One of the means of survey distribution employed was the online channel GoogleDOCS, it was not possible to exactly know how knowledgeable the respondents actually were.

6.6 FUTURE SCOPE OF THE STUDY

Detailed research can be carried out in subsequent studies by other scholars in the future as there are a number of opportunities are available to extend this study. The future scope of the study is as follows:

1. Scholars can do a longitudinal research to compare and contrast the security aspects in the Oil and Gas industry before and after the implementation of the security guidelines identified in this study.
2. In this study, the researcher examined the Oil and Gas industry as the whole value chain and hence there is an opportunity for the researchers to study and recommend the cybersecurity factors in each of the Oil and Gas value chain segments namely Upstream, Midstream and Downstream.
3. Scholars can study the efficacy of the existing Indian cyber law of provisions to understand the suitability of the existing legal framework or suggest

enhancements to enforce the mandatory compliance system recommended in this study.

4. In view of the digitalization / digital transformation happening the Oil and Gas industry, scholars can study the cybersecurity aspects in the Oil and Gas from this new context.

6.7 Concluding Remarks

On the basis of the research study, the researcher was able to identify the four factors that augment the cybersecurity in the Indian Oil and Gas industry. The recommendations and the contribution to the literature were the result of the research that came out with this section. The extension of Laudon and Trevor’s 4-layer security model by including a fifth element of Information Sharing and Collaboration (ISAC) in the Oil and Gas industry was the result of the study. This section also acknowledged the limitations of the current research and provides direction for the scholars to extend the study in the future.

7 APPENDIX

7.1 REFERENCES

REFERENCES

1. A.J. Robb III, H.M. Leith, & J. Piper. (2006). Lessons Learned from Security Vulnerability Assessment Program Implementation in the Petroleum Sector since 9-11. SPE International.

2. Accenture. (2016a). Handling Cyber-attack in Energy Networks- Accenture. Petroleum Review.

3. Accenture. (2016b). Reducing Industrial Cyber Risk in Oil and Gas: Accenture. Retrieved June 2, 2018, from https://www.accenture.com/in-en/insight-highlights-energy-small-ways-make-big-cyber-security

4. Accenture. (2017). Outside the Box - Protecting Core Operations.

5. Allan, K., & Sutton, S. (2015). Oil and gas cybersecurity - time for a seismic shift? Ernst & Young (E&Y).

6. Ananda Kumar, V. (2015). Constituents of the Domain Specific Cybersecurity Mandate for the Indian Power Sector.

7. Ananda Kumar, V., Pandey, K. K., & Punia, D. K. (2014). Cybersecurity threats in the power sector: Need for a domain specific regulatory framework in India. Energy Policy. http://doi.org/10.1016/j.enpol.2013.10.025

8. Andrew Kambour. (2014). State Roles in Enhancing the Cybersecurity of Energy Systems and Infrastructure. National Governors Association.

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

10. ANSSI. (n.d.). Agence nationale de la sécurité des systèmes d'information. Retrieved July 24, 2018, from http://www.ssi.gouv.fr/en/

11. Arcot, R. V. (2015). Is India prepared to protect its critical infrastructure assets from cyber threats? Cyber threat perceptions. CySecurity.

12. Arkkelin, D. (2014). Using SPSS to Understand Research and Data Analysis. Valparaiso University.

13. Babbie, E. R. (2010). The Practice of Social Research 12/e. Belmont, CA: Wadsworth Cengage.

14. Bajpai, S., & Gupta, J. P. (2007). Securing oil and gas infrastructure. Journal of Petroleum Science and Engineering. http://doi.org/10.1016/j.petrol.2006.04.007

15. Bank Info Security. (2017). ONGC CISO on Securing Critical Infrastructure. Retrieved June 2, 2018, from https://www.bankinfosecurity.asia/ongc-ciso-on-securing-critical-infrastructure-a-10296

16. Baudoin, C. R. (2016). Deploying the Industrial Internet in Oil & Gas: Challenges and Opportunities. In SPE Intelligent Energy International Conference and Exhibition. http://doi.org/10.2118/181107-MS

17. Bryman A, & Bell E. (2015). Business Research Methods. Oxford University Press.

18. Bulmer, M. (1984). Facts, Concepts, Theories and Problems. In Sociological Research Methods (pp. 37–50). London: Macmillan Education UK. http://doi.org/10.1007/978-1-349-17619-9_2

19. Business Advantage. (2017). The State of Industrial Cybersecurity 2017.

20. C.R.Kothari. (2004). Research Methodology Methods and Techniques. New Age International (P) Ltd., Publishers.

21. Candid Wueest. (2014). Targeted Attacks against the Energy Sector.

22. Cattell, R. B. (1978). The Scientific Use of Factor Analysis in Behavioral and Life Sciences. Boston, MA: Springer US. http://doi.org/10.1007/978-1-4684-2262-7

23. Centre for Protection of National Infrastructure, U. (2018). Critical National Infrastructure. Retrieved June 19, 2018, from https://www.cpni.gov.uk/critical-national-infrastructure-0

24. CERT.at. (n.d.). Overview - CERT.at. Retrieved July 25, 2018, from https://www.cert.at/index_en.html

25. Chemical Facility Anti-Terrorism Standards | Homeland Security. (n.d.). Retrieved July 8, 2018, from https://www.dhs.gov/chemical-facility-anti-terrorism-standards

26. Chris Dalby. (2016). Cyber insurance is essential for oil companies | Eniday. Retrieved June 2, 2018, from https://www.eniday.com/en/sparks_en/cyber-insurance-for-oil-companies/

27. Chris Hart. (1998). Doing a Literature Review. SAGE Publications.

28. Christopher Bronk, E. T. R. (2013). Hack or Attack? Shamoon and the evolution of Cyber Conflict.

29. Ciepiela, P. (2017). Digitization and cyber disruption in oil and gas.

30. CIO.COM. (n.d.). 2015 State of the CIO: The Good, the Bad and the Scary. Retrieved July 25, 2018, from https://www.cio.com/article/2866469/cio-role/2015-state-of-the-cio-the-good-the-bad-and-the-scary.html

31. CISO Platform. (2017). Top Threats & Controls for IIoT Security. Retrieved June 2, 2018, from http://www.cisoplatform.com/profiles/blogs/highlights-of-panel-discussion-top-threats-amp-controls-for-iiot

32. Cooper, H. M. (1988). Organizing knowledge syntheses: A taxonomy of literature reviews. Knowledge in Society, 1(1), 104–126. http://doi.org/10.1007/BF03177550

33. Costello, A. B., & Osborne, J. W. (2005, July). Practical Assessment, Research and Evaluation (PARE), 10(7).

34. Critical National Infrastructure. (n.d.). Retrieved July 7, 2018, from https://www.cpni.gov.uk/critical-national-infrastructure-0

35. Cyber, D. (2015). Cyber Strategy. U.S. Department of Energy.

36. CyberWiser. (n.d.). Austria (AU). Retrieved July 16, 2018, from https://www.cyberwiser.eu/austria-au

37. CYWARE. (2017). HPCL - Is the Website Under Cerber Ransomware Attack? Retrieved July 15, 2018, from https://cyware.com/news/hpcl-is-the-website-under-cerber-ransomware-attack-6919388d

38. DataBreaches.net. (2015). Two former employees of Essar Refinery accused of data theft. Retrieved May 20, 2018, from https://www.databreaches.net/in-two-former-employees-of-essar-refinery-accused-of-data-theft/

39. Deepak Kumar Sahu. (2017). Cybersecurity Handbook 2017 - Resource Guide on Cybersecurity. Kalinga Digital Media.

40. Department of Energy - USA. (2014). Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2).

41. Department of Homeland Security. (2016). Cybersecurity Overview. Retrieved June 19, 2018, from https://www.dhs.gov/cybersecurity-overview

42. Department of Homeland Security, NCCIC, & ICS-CERT. (2015). NCCIC/ICS-CERT Year in Review (2015).

43. Dexter, J. H. (2002). The Cybersecurity Management System - A Conceptual Mapping. The SANS Institute.

44. DGH. (2016). Evolution of Indian Oil and Gas Industry | Directorate General of Hydrocarbons (DGH).

45. DNG-ISAC. (2018). Downstream Natural Gas ISAC. Retrieved July 15, 2018, from https://www.dngisac.com/

46. DNV-GL. (2015). Cybersecurity vulnerabilities for the oil and gas industry-DNV GL. Retrieved June 2, 2018, from https://www.dnvgl.com/oilgas/download/lysne-committee-study.html

47. Downstream Natural Gas ISAC. (n.d.). Retrieved July 8, 2018, from https://www.isao.org/information-sharing-group/sector/downstream-natural-gas-isac/

48. Dr, S. G. (2008). Business Research Methods.

49. Dragos. (2017a). Industrial Control System Threats.

50. Dragos. (2017b). Industrial Control Vulnerabilities.

51. Dziuban, C. D., & Shirkey, E. C. (1974, Jun). When is a correlation matrix appropriate for factor analysis? Psychological Bulletin, 81(6), 358-361.

52. Economic Times CISO. (2017). Oil and Gas Companies are partially aware of cyber analytics technology to monitor cyberattacks says Accenture research, IT Security News, ET CISO. Retrieved June 2, 2018, from https://ciso.economictimes.indiatimes.com/news/oil-and-gas-companies-are-partially-aware-of-cyber-analytics-technology-to-monitor-cyberattacks-says-accenture-research/58065998

53. EECSP. (2017). Cyber Security in the Energy Sector Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector.

54. EE-ISAC. (n.d.). It’s crucial to look beyond segment borders... Retrieved July 25, 2018, from http://www.ee-isac.eu/about

55. E-ISAC. (2017). Modular ICS Malware. E-ISAC.

56. Elbaradie, M. (2017). Critical Controls for Effective Cyber Defense. World Petroleum Council.

57. ENCS. (n.d.). European Network for Cyber Security. Retrieved July 25, 2018, from https://encs.eu/

58. ENISA. (2011). Protecting Industrial Control Systems.

59. ENISA. (2016). Incident Reporting Framework.

60. ENISA. (n.d.). ICS SCADA — ENISA. Retrieved July 25, 2018, from https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/scada

61. ENISA. (2017). Report on Cybersecurity Information Sharing in the Energy Sector About ENISA Report on Cybersecurity Information Sharing in the Energy Sector Corrigendum Notice Report on Cybersecurity Information Sharing in the Energy Sector. Retrieved from https://www.enisa.europa.eu/publications/information-sharing-in-the-energy-sector

62. Ernst & Young (EY). (2015). Creating trust in the digital world EY's Global Information Security Survey 2015 Power and utilities sector results.

63. European Commission. (n.d.). Critical Infrastructure Warning Information Network (CIWIN). Retrieved July 25, 2018, from https://ec.europa.eu/home-affairs/what-we-

do/networks/critical_infrastructure_warning_information_network_en

64. European Commission. (2012). Position Paper of the TNCEIP on EU Policy on Critical Energy Infrastructure Protection (November 2012).

65. Everitt, B. S. (1975). Multivariate Analysis: the Need for Data, and other Problems. The British Journal of Psychiatry, 126(3), 237–240. http://doi.org/10.1192/bjp.126.3.237

66. Express Computer. (2017). The digital assets at IOCL have grown multifold. Retrieved June 2, 2018, from http://computer.expressbpd.com/news/the-digital-assets-at-iocl-have-grown-multifold/23030/

67. Exxonmobil. (2010). Corporate Citizenship Report - Exxonmobil 2010.

68. Farooq Shaik, Arif Abdullah, S. K. (2017). Digital Transformation in Oil and Gas - Cybersecurity and Approach to Safeguard Your Business. 22nd World Petroleum Congress.

69. FIRST. (n.d.). Statoil CSIRT. Retrieved July 16, 2018, from https://www.first.org/members/teams/statoil_csirt

70. Ganesh Ramamoorthy. (2015). Gartner's take on the Indian IoT Landscape. Retrieved July 9, 2018, from https://enterprise-security.cioreviewindia.com/cxoinsight/gartner-s-take-on-the-indian-iot-landscape-nid-3037-cid-52.html

71. Gartner Inc. (2018). Operational Technology (OT) - Gartner IT Glossary. Retrieved May 21, 2018, from https://www.gartner.com/it-glossary/operational-technology-ot/

72. Garvin, T. (2015). IT and OT Convergence, or Collision? Managing the Merger for Greenfield LNG. Society of Petroleum Engineers.

73. Gaskin. (2012a). Confirmatory Factor Analysis - StatWiki. Retrieved May 21, Statwiki (2018). from http://statwiki.kolobkreations.com/index.php?title=Confirmatory_Factor_Analysis

74. Gaskin. (2012b). Exploratory Factor Analysis - StatWiki. Retrieved May 21, 2018, from http://statwiki.kolobkreations.com/index.php?title=Exploratory_Factor_Analysis

75. Glen D. Israel. (2003). Determining Sample Size.

76. Goodman, M. (2015). Future Crimes. Doubleday

77. Gorsuch, R. L. (1988). Exploratory Factor Analysis. In Handbook of Multivariate Experimental Psychology (pp. 231–258). Boston, MA: Springer US. http://doi.org/10.1007/978-1-4613-0893-5_6

78. Government of India. (2000). Information Technology Act 2000. Government of India, 19.

79. Greenacre, M. J., & Primicerio, R. (2013). Multivariate analysis of ecological data. Fundación BBVA. Retrieved from http://www.multivariatestatistics.org/

80. Gregory Hale. (2016). Cybersecurity attacks against oil and gas organizations increasing. Retrieved May 20, 2018, from

https://www.oilandgaseng.com/singlearticle/cyber-security-attacks-against-oil-and-gas-organizations-increasing/23b39f2b2b49675e3f4e5c40796f974c.html

81. GCSC. (n.d.). The European SCADA and Control System Information Exchange. Retrieved July 24, 2018, from https://www.gcsec.org/blog/european-scada-control-system-information-exchange

82. Gupta, M., Bhattacharya, J., & Chaturvedi, M. M. (2009). Cybersecurity Infrastructure in India: A Study. Retrieved from https://www.researchgate.net/publication/228846974

83. Hair, J. F. (2010). Multivariate data analysis. Prentice Hall.

84. Hellstrom, T. (2007). Critical infrastructure and systemic vulnerability: Towards a planning framework. Safety Science. http://doi.org/10.1016/j.ssci.2006.07.007

85. Hooper, D., Mullen, J., Hooper, D., Coughlan, J., & Mullen, M. R. (2008). Structural Equation Modelling: Guidelines for Determining Model Fit.

86. Hu, L.-t., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. Structural Equation Modelling: A Multidisciplinary Journal, 6(1), 1-55.

87. IDSA. (2012). India’s Cybersecurity Challenges - IDSA Taskforce Report. Retrieved from http://www.idsa.in

88. INGAACoverandComments. (2009). INGAA.

89. Infrastructure. (n.d.). Retrieved July 7, 2018, from

https://www.sciencedaily.com/terms/infrastructure.htm

90. International Association of Drilling Contractors. (2018). IADC Cybersecurity Overview. International Association of Drilling Contractors.

91. ISO-IEC. (2012). National Cybersecurity Policy -2013.

92. Jason Holcomb. (2016). Definitive Guide to Cybersecurity for the Oil & Gas Industry. Leidos.

93. Jason, T. M. C. (2010). Science of Cyber-Security.

94. Jennifer Rockwood, S. C. M. (2015). The Digital Future is now: Executive Talent Implications of Digital in Oil & Gas. Retrieved June 19, 2018, from http://www.russellreynolds.com/newsroom/the-digital-future-is-now-executive-talent-implications-of-digital-in-oil-gas

95. Jeremy Fleming. (2013). EU, US go separate ways on cybersecurity – EURACTIV.com. Retrieved May 21, 2018, from https://www.euractiv.com/section/cybersecurity/news/eu-us-go-separate-ways-on-cybersecurity/

96. Joel Parshall. (2018). Cyber Attacks Pose Increasing Industry Threat. JPT.

97. Johnson, C. S., Badger, M. L., Waltermire, D. A., Snyder, J., & Skorupka, C. (2016). Guide to Cyber Threat Information Sharing.

98. Kim Zetter. (2010). Critical Infrastructures Under Constant Cyberattack Globally. Retrieved May 21, 2018, from https://www.wired.com/2010/01/csis-report-on-cybersecurity/

99. Klahr, R., Amili, S., Shah, J. N., Button, M., & Wang, V. (2016). Cybersecurity Breaches Survey 2016.

100.Knapp, D. E., & Langill, J. T. (2015). Industrial Network Security, Second Edition. Waltham, MA: Syngress.

101.KraftCERT. (n.d.). KraftCERT is working for more secure and robust ICS systems by assisting the energy sector. Retrieved July 25, 2018, from https://www.kraftcert.no/english/index.html

102.KRITIS. (n.d.). Cyber Security Strategy for Germany. Retrieved July 25, 2018, from https://www.kritis.bund.de/SubSites/Kritis/EN/publications/Cyber-Security-Stategy.html

103.Kroger, W. (2008). Critical infrastructures at risk - A need for a new conceptual approach and extended analytical tools. Reliability Engineering and System Safety. http://doi.org/10.1016/j.ress.2008.03.005

104.Lalanne, C. (n.d.). Comments on statistical validity of factor analysis. Retrieved Jan 26, 2014, from Aliquote.org: http://www.aliquote.org/articles/tech/multvar/22_Appendix_6.pdf

105.Laudon & Trever. (2014). E-Commerce - Business, Technology, Society. Pearson.

106.Lewis, J. A. (2013). Raising the Bar for Cybersecurity.

107.Liang, X., & Xiao, Y. (2013). Game Theory for Network Security. Communications Surveys & Tutorials, IEEE, 15(1), 472-486.

108.MacCallum, R. C., Widaman, K. F., Zhang, S., & Hong, S. (1999). Sample size in factor analysis. American Psychological Association. http://doi.org/10.1037/1082-989X.4.1.84

109.MacDougall, C., & Fudge, E. (2001, Jan). Pearls, Pith, and Provocation: Planning and Recruiting the Sample for Focus Groups and In-Depth Interviews. Qualitative Health Research, 11(1), 117-126.

110.Malhotra, N. K. (2010). Marketing research : an applied orientation. Pearson.

111.McKinsey & Company. (2014). Why senior leaders are the front line against cyberattacks. Retrieved May 20, 2018, from https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/why-senior-leaders-are-the-front-line-against-cyberattacks

112.Messick, S. (1980). Test Validity and the ethics of assessment. American Psychologist, 35, 1012-1027.

113.Minichiello, V., Aroni, R., Hays, T., Pearson, E., & Hall, P. (2014). In-depth Interviewing. Pearson. Retrieved from www.pearsoned.com.au

114.Ministry of Telecommunications. (2012). National Telecom Policy 2012.

115.Mischa Hansel. (2013). Cybersecurity Governance and the Theory of Public Goods. Retrieved May 21, 2018, from http://www.e-ir.info/2013/06/27/cyber-security-governance-and-the-theory-of-public-goods/

116.Moore, D. A. (2013). Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries. Journal of Loss Prevention in the Process

Industries. http://doi.org/10.1016/

117.MOPNG. (n.d.). India’s new Hydrocarbon Exploration and Licensing Policy (HELP) launch at CERA Week 2017 | Ministry of Petroleum and Natural Gas. Retrieved July 25, 2018, from http://petroleum.nic.in/india’s-new-hydrocarbon-exploration-and-licensing-policy-help-launch-cera-week-2017

118.Moumita Samanta. (2018). India’s Energy Demand to Double by 2035. Retrieved July 25, 2018, from http://www.advisorymandi.com/editors-pick/INDUSTRY-UPDATEINDIAS-ENERGY-DEMAND-TO-DOUBLE-BY-2035-135

119.Muktesh Chander. (2014). NCIIPC Role, Charter & Responsibilities. NTRO.

120.Najoua Aarab, Siv Hilde Houmb, Kent Hulick, & Erlend A. Engum. (2014). Process for Security Policy and Requirements Development. Society of Petroleum Engineers This.

121.National Institute of Standards and Technology (NIST). (2017). Framework for Improving Critical Infrastructure Cybersecurity. Infrastructure Cybersecurity Draft Version 1.1 National Institute of Standards and Technology.

122.Nasir, M. A., Sultan, S., Nefti-Meziani, S., & Manzoor, U. (2015). Potential cyber-attacks against global oil supply chain. In International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA) 2015. http://doi.org/10.1109/CyberSA.2015.7166137

123.Nathan Zhao. (2009). The Minimum Sample Size in Factor Analysis. Retrieved May 21, 2018, from https://www.encorewiki.org/display/~nzhao/The+Minimum+Sample+Size+in+

Factor+Analysis

124.National Institute of Standards and Technology. (2017). Framework for Improving Critical Infrastructure Cybersecurity. Infrastructure Cybersecurity Draft Version 1.1 National Institute of Standards and Technology.

125.NCIIPC. (2013). Guidelines for Protection of National Critical Information Infrastructure.

126.Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of cyber-warfare. Computers and Security. http://doi.org/10.1016/j.cose.2012.02.009

127.Nolan, A. (2015). Cybersecurity and Information Sharing - Legal Challenges and Solutions. Congressional Research Service.

128.NSSC. (n.d.). Nationaal Cyber Security Centrum. Retrieved July 16, 2018, from https://www.ncsc.nl/

129.ONG-ISAC. (2016). Oil and Natural Gas Information Sharing and Analysis Center. Retrieved May 20, 2018, from http://www.ongisac.org/

130.Onyeji, I., Bazilian, M., & Bronk, C. (2014). Cybersecurity and critical energy infrastructure. The Electricity Journal. http://doi.org/10.1016/j.tej.2014.01.011

131.Ponemon Institute. (2016). Cost of Cyber Crime Study & the Risk of Business Innovation.

132.Ponemon Institute. (2017a). Cost of Data Breach Study Global Overview 2017 Cost of Data Breach Study: Global Overview.

133.Ponemon Institute. (2017b). The State of Cybersecurity in the Oil & Gas Industry -United States.

134.Prasenj Saha. (2018). The Growing Risks of Cybersecurity Breach: Oil & Gas Perspective | LTI. Retrieved June 2, 2018, from https://www.lntinfotech.com/blogs/the-growing-risks-of-cyber-security-breach-oil-gas-perspective/

135.Price Waterhouse Coopers. (2013). Embedding cybersecurity into the energy ecosystem - An integrated approach to assessing cyber threats and protecting your assets.

136.Price Waterhouse Coopers. (2017). Bold steps to manage geopolitical threats final.

137.Randolph, J. J. (2009). A Guide to Writing the Dissertation Literature Review - Practical Assessment, Research & Evaluation, 14(13).

138.Reuters. (2017). Statoil moves key IT tasks from India back to Norway | Reuters. Retrieved June 19, 2018, from https://www.reuters.com/article/statoil-norway-cyber-idUSL8N1JR41E

139.Rick, K., & Iyer, K. (2016). Countering the threat of Cyberattacks in oil and gas.

140.RiskWatch. (2012). Oil and Gas Industry A Comprehensive Security Risk Management Approach. Retrieved from www.riskwatch.com

141.Ryu, D. H., Kim, H., & Um, K. (2009). Reducing security vulnerabilities for critical infrastructure. Journal of Loss Prevention in the Process Industries.

http://doi.org/10.1016/j.jlp.2009.07.015

142.Saikat Datta. (2016). The Development and Role of the National Critical Information Infrastructure Protection Centre (NCIIPC).

143.Sameer Patil. (2014). India’s vulnerable SCADA systems. Retrieved May 21, 2018, from http://www.gatewayhouse.in/indias-vulnerable-scada-systems/

144.Schreiber, J. B., Nora, A., Stage, F. K., Barlow, E. A., & King, J. (2006). Reporting Structural Equation Modeling and Confirmatory Factor Analysis Results: A Review. The Journal of Educational Research, 99(6), 323-338.

145.Schutte, N., Toppinnen, S., Kalimo, R., & Schaufeli, W. (2000). The Factorial Validity of the Maslach Burnout Inventory - General Survey across Occupational Groups and Nations. Journal of Occupational and Organizational Psychology, 73(1), 53 – 67

146.Sharma, M. (2017). Securing Critical Information Infrastructure - Global Perspectives and Practices. Institute for Defense Studies and Analyses.

147.Shiva, S., Roy, S., & Dasgupta, D. (2010). Game Theory for Cybersecurity.

148.SI-CERT. (n.d.). SI-CERT (Slovenian Computer Emergency Response Team) is the national cyber scurity incident response center. Retrieved July 25, 2018, from https://www.cert.si/en/

149.Statistics Solution. (2013). Confirmatory Factor Analysis. Retrieved Jan 26, 2015, from Statistics Solution: http://www.statisticssolutions.com/academicsolutions/resources/directory-of-statistical-analyses/confirmatoryfactor-analysis/

150.Steiger, J. H. (n.d.). Path Diagrams. Retrieved Jan 26, 2015, from Statpower: http://www.statpower.net/Content/GCM/Handouts/Path%20Diagrams. pdf

151.Systems and Network Analysis Center, National Security Agency. (2010, Aug 20). A Framework for Assessing and Improving the Security Posture of Industrial Control Systems (ICS). Retrieved from NSA.GOV: https://www.nsa.gov/ia/_files/ics/ics_fact_sheet.pdf

152.Tai, K., Kizhakkedath, A., Lin, J., Tiong, R. L. K., & Sim, M. S. (2013). Identifying Extreme Risks in Critical Infrastructure Interdependencies. International Symposium for Next Generation Infrastructure. http://doi.org/10.14453/isngi2013.proc.44

153.Taro Yamane. (1973). Statistics: An Introductory Analysis. Retrieved from https://www.amazon.com/Statistics-Introductory-Analysis-Taro-Yamane/dp/0063565722

154.Taryn Aguas, Khalid Kark, & Monique François. (2016). The new CISO Leading the strategic security organization.

155.The Economic Times. (2014). Indian Oil Corp website hacked by a Turkish group. Retrieved May 20, 2018, from https://economictimes.indiatimes.com/industry/energy/oil-gas/indian-oil-corp-website-hacked-by-a-turkish-group/articleshow/45706026.cms

156.The Economic Times. (2017). Over 53,000 cybersecurity incidents observed in 2017 - The Economic Times. Retrieved June 19, 2018, from https://economictimes.indiatimes.com/tech/ites/over-53000-cyber-security-incidents-observed-in-2017/articleshow/62852008.cms

157. The Electronic Journal of Business Research Methods, 6(1), 53–60. Retrieved from www.ejbrm.com

158. The Gazette of India. (2014). National Critical Information Ifrastructure Protection Centre.

159. The Hindu. (2013). Petroleum Ministry warns PSU oil companies of cyber-attacks. Retrieved May 20, 2018, from http://www.thehindu.com/business/Industry/petroleum-ministry-warns-psu-oil-companies-of-cyber-attacks/article5394215.ece

160. The Indian Express. (2015). Identity theft - ONGC falls prey to cyber fraud, loses Rs.197 crore | The Indian Express. Retrieved May 20, 2018, from http://indianexpress.com/article/business/companies/identity-theft-ongc-falls-prey-to-cyber-fraud-loses-rs-197-crore/

161. Tim Haidar. (2015). Oil and Gas Cybersecurity: The Mammoth Cost Of Not Being Prepared. Oil & Gas IQ.

162. Tim Lester. (2016). Cybersecurity - A growing threat to the energy sector - An Australian perspective.

163. Tiwari, U. (2016). A Report on the Indian Computer Emergency Response Team’s Proactive Mandate in the Indian Cybersecurity Ecosystem. The Centre for Internet & Society.

164. Transparency Market Research. (2016). Oil and Gas Cybersecurity Market - Global Industry Analysis, Size, Share, Growth, Trends, and Forecast 2016 - 2024. Retrieved June 19, 2018, from

https://www.transparencymarketresearch.com/oil-gas-cyber-security-market.html

165.Tripwire. (2016). Identifying Cyber Risks - The Important Role of Senior Management. Retrieved May 20, 2018, from https://www.tripwire.com/state-of-security/risk-based-security-for-executives/risk-management/identifying-cyber-risks-the-important-role-of-senior-management/

166.U.S. Department of Homeland Security. (2004). A Comparison of Oil and Gas Segment Cybersecurity Standards. U.S. Department of Homeland Security.

167.US Government Publishing Office. (1998). Presidential Decision Directive 63 on Critical Infrastructure Protection: Sector Coordinators. Retrieved June 19, 2018, from https://fas.org/irp/offdocs/pdd/pdd-63.htm

168.Velda Addison. (2015). Information Sharing Is Key to Cybersecurity | Exploration & Production. Retrieved June 19, 2018, from https://www.epmag.com/information-sharing-key-cyber-security-827031

169.Willis. (2014). Energy Market Reviews 2014 Cyber Attacks - Can the Market Respond?

170.Yi Luo, F. S.-N. (2010). Game Theory Based Network Security. Scientific Research, 41 - 44.

171.Yunis, M. M., & Koong, K. S. (2015). A Conceptual Model for the Development of a National Cybersecurity Index: An Integrated Framework. Twenty First Americans Conference on Information Systems.

172.Zheng, D. E., & Lewis, J. A. (2015). Cyber Threat Information Sharing:

Recommendations for Congress and the Administration. Centre for Strategic and International Studies.

7.2 QUESTIONNAIRE – SEMI STRUCTURED

(For finalizing variables from interview)

Thank you for taking time to answer a set of questions. Your exact identity will not be captured.

Name: ____

Designation: ____

Company: ____

Date: ____

- **Risk Management**
  - Should Oil and Gas industry conduct a baseline cybersecurity risk assessment and arrive at a risk score?
  - Are periodic Industry wide cybersecurity drills conducted in the Oil and Gas industry? If so, how frequently?
  - Does the industry ensure third party security assessments on an annual basis in the Oil and Gas industry?
  - Are the cybersecurity risk assessments reviewed periodically?

- **Asset, Change and Configuration Management**
  - How are the organization's IT and OT assets, including both hardware and software from cybersecurity perspective?
  - Do the companies identify and maintain an inventory of its critical cyber-physical assets?
  - Is there a policy of security certifications of products, which are categorized as critical cyber-physical assets?
  - How about logging every changes to the cyber-physical assets?

- **Identity and Access Management**
    - How is the creation and management of identities for entities that may be granted logical and physical access to the organization's assets?
    - How soon identities are removed when someone quits the organization?
    - Are the credentials periodically reviewed to ensure that they are associated with the correct person or entity?
    - Is the access to cyber physical assets revoked when no longer required?

- **Threat and Vulnerability Management**
    - How plans, procedures and technologies are managed and maintained to detect, identify, analyze, manage and respond to cybersecurity threats and vulnerabilities?
    - Is there a practice of collecting useful information from reliable sources like Industry Associations, Computer Emergency Response Team (CERT) etc.?
    - How frequently are vulnerability information is collected and analyzed using scanning tools, penetration tests, and cybersecurity tests?
    - Are stakeholder's identified and involved for threat and vulnerability management activities?

- **Information Sharing and Communications**
    - How is the relationship with internal and external entities established and maintained to collect and provide cybersecurity information, including threats and vulnerabilities to reduce risks and to increase operational resilience?
    - Is there a need to set up an Oil and Gas industry specific collaboration forum to share security knowledge, incidents and best practices?
    - Are disclosure of breaches and security incidents shared with a nodal agency been done regularly?

- Is it important for the nodal agency to main a current directory of industry-wide cybersecurity emergency response contacts?

- **Workforce Management**
  - How plans, procedures, technologies and controls are established and maintained to create a culture of cybersecurity and to ensure the ongoing suitability and competency of personnel?
  - Is there a plan for the company to identify and nominate a senior executive (like Chief Information Security Officer - CISO) who would be reporting to the Board?
  - Are cybersecurity education and training made mandatory for all employees in the Oil and Gas industry?
  - Are employees working in or having access to sensitive domains screened and security cleared?

- **Cybersecurity Program Management**
  - How an enterprise cybersecurity program is established and maintained that provides governance, strategic planning and sponsorship for the organization's cybersecurity activities?
  - Is there a cyber-security program strategy that includes a list of cybersecurity objectives and a plan to meet them?
  - Is sponsorship from senior management important for implementing the cybersecurity program for providing resources like People, Tools and Funding?

- **Others**
  - In your opinion, what other aspects of cybersecurity or governance should be included in the national cybersecurity policy for the Oil and Gas industry in India?

7.3 QUESTIONNAIRE – STRUCTURED

Thank you for taking time to answer a set of questions. Your exact identity will not be captured. So please feel free to respond to the best of your belief and conviction. The data collected will be used only for my Research work and will not be shared with any third party. It is likely to take about 10 minutes to complete this questionnaire.

How would you describe yourself?

- Decision Makers - Policy Maker / Government Sector / Academician
- Leaders of the Oil and Gas Industry - CIOs, CISOs
- Practitioners - IT Managers
- Facilitators - System Integrators - Security professional - Security Auditor

How would you describe your industry?

- Upstream
- Midstream
- Downstream
- Integrated Oil and Gas
- Oil Field Services
- EPC Company
- Security Service Provider / System Integrator
- Government Bodies / Independent Bodies / Academic Institutions / Research Institution/ Analysts

For the questions below, please choose (on the 5 point scale) your response based on **whether the variable proposed would increase Cybersecurity in Indian Oil and Gas Industry.** Please 'tick' or 'circle' your response on the choice. For example: Agree

1. ***Oil and Gas industry should conduct a baseline cybersecurity risk assessment and arrive at a risk score.***

○	Strongly Disagree
○	Disagree
○	Neither Agree nor Disagree
○	Agree
○	Strongly Agree

2. Periodic Industry wide cybersecurity drills should be conducted in the Oil and Gas industry.

○	Strongly Disagree
○	Disagree
○	Neither Agree nor Disagree
○	Agree
○	Strongly Agree

3. Third party security assessments should be made mandatory on an annual basis in the Oil and Gas industry

○	Strongly Disagree
○	Disagree
○	Neither Agree nor Disagree
○	Agree
○	Strongly Agree

4. Cybersecurity risk assessments should be reviewed periodically.

○	Strongly Disagree
○	Disagree
○	Neither Agree nor Disagree
○	Agree
○	Strongly Agree

5. Organization should identify and maintain an inventory of its critical cyber-physical assets.

○	Strongly Disagree
○	Disagree
○	Neither Agree nor Disagree
○	Agree
○	Strongly Agree

6. There is a need to enforce security certifications of products that are categorized as critical cyber-physical assets.

○	Strongly Disagree
○	Disagree
○	Neither Agree nor Disagree
○	Agree

○	Strongly Agree

7. Every changes to the cyber-physical assets should be logged.

○	Strongly Disagree
○	Disagree
○	Neither Agree nor Disagree
○	Agree
○	Strongly Agree

8. Establishing and maintaining identities should begin with the provisioning and de-provisioning of identities to entities. (Removing identities when someone quits the organization)

○	Strongly Disagree
○	Disagree
○	Neither Agree nor Disagree

○	Agree
○	Strongly Agree

9. Credentials should be periodically reviewed to ensure that they are associated with the correct person or entity.

○	Strongly Disagree
○	Disagree
○	Neither Agree nor Disagree
○	Agree
○	Strongly Agree

10. Access to cyber physical assets should be revoked when no longer required.

○	Strongly Disagree
○	Disagree
○	Neither Agree nor Disagree

○	Agree
○	Strongly Agree

11. Threat identification and response should begin with collecting useful information from reliable sources like Industry Associations, CERT etc.

○	Strongly Disagree
○	Disagree
○	Neither Agree nor Disagree
○	Agree
○	Strongly Agree

12. Reducing cybersecurity vulnerabilities should begin with collecting and analyzing vulnerability information using scanning tools, penetration tests, and cybersecurity tests.

○	Strongly Disagree
○	Disagree

○	Neither Agree nor Disagree
○	Agree
○	Strongly Agree

13. Stakeholders should be identified and involved for threat and vulnerability management activities.

○	Strongly Disagree
○	Disagree
○	Neither Agree nor Disagree
○	Agree
○	Strongly Agree

14. Here is a need to set up an Oil and Gas industry specific collaboration forum to share security knowledge, incidents and best practices.

○	Strongly Disagree

○	Disagree
○	Neither Agree nor Disagree
○	Agree
○	Strongly Agree

15. Disclosure of breaches and security incidents to a nodal agency should be made mandatory for companies in the Oil and Gas industry.

○	Strongly Disagree
○	Disagree
○	Neither Agree nor Disagree
○	Agree
○	Strongly Agree

16. It is important for the nodal agency to main a current directory of industry wide cybersecurity emergency response contacts

○	Strongly Disagree
○	Disagree
○	Neither Agree nor Disagree
○	Agree
○	Strongly Agree

17. Organization should identify and nominate a senior executive (like Chief Information Security Officer - CISO) who would be reporting to the Board.

○	Strongly Disagree
○	Disagree
○	Neither Agree nor Disagree
○	Agree
○	Strongly Agree

18. Cybersecurity education and training should be made mandatory for all employees in the Oil and Gas industry

○	Strongly Disagree
○	Disagree
○	Neither Agree nor Disagree
○	Agree
○	Strongly Agree

19. Employees working in or having access to sensitive domains should be screened and security cleared.

○	Strongly Disagree
○	Disagree
○	Neither Agree nor Disagree
○	Agree
○	Strongly Agree

20. A Cybersecurity program strategy should include a list of cybersecurity objectives and a plan to meet them.

○	Strongly Disagree
○	Disagree
○	Neither Agree nor Disagree
○	Agree
○	Strongly Agree

21. Sponsorship is important for implementing the cybersecurity program for providing resources like People, Tools and Funding.

○	Strongly Disagree
○	Disagree
○	Neither Agree nor Disagree
○	Agree

○	Strongly Agree

In your opinion, what other aspects of cybersecurity or governance should be included in the national cybersecurity policy for the Oil and Gas industry in India

7.4 LITERATURE REVIEW UNDER THEMES

S.No	Title	Author & Year	Theme
1	Presidential Decision Directive 63 on Critical Infrastructure Protection: Sector Coordinators	US Government Publishing Office	National Critical Infrastructure
2	Cybersecurity Overview	Department of Homeland Security, USA	National Critical Infrastructure
3	Critical National Infrastructure	Centre for Protection of National Infrastructure, UK	National Critical Infrastructure
4	Information Technology Act 2000	Government of India	National Critical Infrastructure
5	Critical Infrastructures Under Constant Cyberattack Globally	Kim Zetter (2010)	Critical Infrastructure Under Threat
6	Critical infrastructures at risk - A need for a new conceptual approach and extended analytical tools	Kroger, W. (2008)	Critical Infrastructure Under Threat

7	Cybersecurity and critical energy infrastructure	Onyeji, I., Bazilian, M., & Bronk, C. (2014)	Critical Infrastructure Under Threat
8	Securing Critical Information Infrastructure - Global Perspectives and Practices	Sharma, M. (2017)	Critical Infrastructure Under Threat
9	Reducing security vulnerabilities for critical infrastructure	Ryu, D. H., Kim, H., & Um, K. (2009)	Critical Infrastructure Under Threat
10	Identifying Extreme Risks in Critical Infrastructure Interdependencies	Tai, K., Kizhakkedath, A., Lin, J., Tiong, R. L. K., & Sim, M. S. (2013)	Critical Infrastructure Under Threat
11	Critical infrastructure and systemic vulnerability: Towards a planning framework	Tomas Hellstrom (2006)	Critical Infrastructure Under Threat
12	SCADA security in the light of Cyber-Warfare	Andrew Nickolson et all 2012	Critical Infrastructure Under Threat
13	Oil and Gas Cybersecurity Market - Global Industry	Transparency Market Research (2016)	Critical Infrastructure Under Threat

	Analysis, Size, Share, Growth, Trends, and Forecast 2016 - 2024		
14	Reducing Industrial Cyber Risk in the Petroleum Sector	Accenture. (2016)	Cyber Threats in Oil and Gas
15	Handling Cyber-attack in Energy Networks	Accenture. (2016)	Cyber Threats in Oil and Gas
16	Outside the Box - Protecting Core Operations	Accenture. (2017).	Cyber Threats in Oil and Gas
17	Cybersecurity vulnerabilities for the oil and gas industry	DNV-GL. (2015)	Cyber Threats in Oil and Gas
18	Embedding cybersecurity into the energy ecosystem - An integrated approach to assessing cyber threats and protecting your asset	Price Waterhouse Coopers (2013)	Cyber Threats in Oil and Gas
19	Bold steps to manage geopolitical threats final	Price Waterhouse Coopers (2017)	Cyber Threats in Oil and Gas
20	Oil and Gas Industry A Comprehensive	RiskWatch (2012)	Cyber Threats in Oil and Gas

	Security Risk Management Approach		
21	Targeted Cyber Attacks Against the Energy Sector	Candid Wueest (2014)	Cyber Threats in Oil and Gas
22	Cyber insurance is essential for oil companies	Chris Dalby (2016)	Cyber Threats in Oil and Gas
23	Hack or Attack? Shamoon and the evolution of Cyber Conflict	Christopher Bronk, E. T. R. (2013)	Cyber Threats in Oil and Gas
24	Lessons Learned from Security Vulnerability Assessment Program Implementation in the Petroleum Sector since 9/11	A.J. Robb III, H.M. Leith, & J. Piper. (2006)	Cyber Threats in Oil and Gas
25	Oil and Gas Companies are partially aware of cyber analytics technology to monitor cyberattacks	Economic Times CISO. (2017)	Cyber Threats in Oil and Gas
26	Critical Controls for Effective Cyber	Elbaradie, M. (2017)	Cyber Threats in Oil and Gas

	Defense. World Petroleum Council		
27	Cybersecurity attacks against oil and gas organizations increasing	Gregory Hale. (2016)	Cyber Threats in Oil and Gas
28	IADC Cybersecurity Overview	International Association of Drilling Contractors. (2018)	Cyber Threats in Oil and Gas
29	The Growing Risks of Cybersecurity Breach: Oil & Gas Perspective	Prasenj Saha Lntinfortech (LTI). (2018)	Cyber Threats in Oil and Gas
30	Potential cyber-attacks against global oil supply chain	Nasir Sultan, S., Nefti-Meziani, S., & Manzoor, U. (2015)	Cyber Threats in Oil and Gas
31	Cyber 9/11: Is the Oil & Gas Industry Sleepwalking into a Nightmare?	Tim Haidar (2015)	Cyber Threats in Oil and Gas
32	Corporate Citizenship Report - Exxonmobil 2010	ExxonMobil (2010)	Cyber Threats in Oil and Gas
33	Energy Market Reviews 2014 Cyber Attacks -	Willis. (2014)	Cyber Threats in Oil and Gas

	Can the Market Respond?		
34	Process for Security Policy and Requirements Development	Najoua Aarab, Siv Hilde Houmb, Kent Hulick, & Erlend A. Engum (2014)	Cyber Threats in Oil and Gas
35	NCCIC/ICS-CERT Year in Review	Department of Homeland Security (2015)	Cyber Threats in Oil and Gas
36	Securing oil and gas infrastructure	S.Bajpai et al (2007)	Cyber Threats in Oil and Gas
37	O&G Prepare to Thrive Despite a Cyber Attack	Booz Allen Hamilton (2015)	Cyber Threats in Oil and Gas
38	NCIIPC Role, Charter & Responsibilities. NTRO	Muktesh Chander (2014)	Cyber Threats in India
39	Guidelines for Protection of National Critical Information Infrastructure	NCIIPC (2013)	Cyber Threats in India
40	The Development and Role of the National Critical Information Infrastructure Protection Centre (NCIIPC)	Saikat Datta (2016)	Cyber Threats in India

41	Cybersecurity Infrastructure in India: A Study	Gupta, M., Bhattacharya, J., & Chaturvedi, M. M. (2009)	Cyber Threats in India
42	India's Cybersecurity Challenges - IDSA Taskforce Report	IDSA. (2012)	Cyber Threats in India
43	India's vulnerable SCADA systems	Sameer Patil (2014)	Cyber Threats in India
44	The digital assets at IOCL have grown multifold	Express Computer (2017)	Cyber Threats in India
45	Identity theft - ONGC falls prey to cyber fraud, loses Rs.197 crore	The Indian Express (2015)	Cyber Threats in India
46	Indian Oil Corp website hacked by a Turkish group	The Economic Times (2014)	Cyber Threats in India
47	Two former employees of Essar Refinery accused of data theft	DataBreaches.net (2015)	Cyber Threats in India
48	Petroleum Ministry warns PSU oil	The Hindu (2013)	Cyber Threats in India

	companies of cyber attacks		
49	Statoil moves key IT tasks from India back to Norway	Reuters (2017)	Cyber Threats in India
50	A Report on the Indian Computer Emergency Response Team’s Proactive Mandate in the Indian Cybersecurity Ecosystem	Tiwari, U. (2016)	Cyber Threats in India
51	Over 53,000 cybersecurity incidents observed in 2017	Economic Times (2018)	Cyber Threats in India
52	Is India prepared to protect its critical Infrastructure assets from cyber threats?	Rajabahadur V. Arcot (2014)	Cyber Threats in India
53	National Telecom Policy 2012	Ministry of Telecommunications. (2012)	Cyber Threats in India
54	Cost of Cyber Crime Study & the Risk of Business Innovation	Ponemon Institute. (2016)	Cost of Cyber Threats

55	Cost of Data Breach Study Global Overview 2017 Cost of Data Breach Study: Global Overview	Ponemon Institute (2017)	Cost of Cyber Threats
56	IT and OT Convergence, or Collision? Managing the Merger for Greenfield LNG	Garvin, T. (2015)	IT-OT Convergence
57	Deploying the Industrial Internet in Oil & Gas: Challenges and Opportunities.	Baudoin, C. R. (2016)	IT-OT Convergence
58	Protecting the connected barrels - Cybersecurity for upstream oil and gas	Anshu Mittal, Andrew Slaughter, & Paul Zonneveld (2017).	IT-OT Convergence
59	Creating trust in the digital world EY's Global Information Security Survey 2015 Power and utilities sector results	Ernst & Young (E&Y). (2015)	IT-OT Convergence
60	The State of Cybersecurity in the Oil	Ponemon Institute (2017)	IT-OT Convergence

	& Gas Industry -United States		
61	Digitization and cyber disruption in oil and gas	Ciepiela, P. (2017)	IT-OT Convergence
62	Cyber Attacks Pose Increasing Industry Threat	Joel Parshall. (2018)	IT-OT Convergence
63	The State of Industrial Cybersecurity 2017	Business Advantage (2017).	Cyber Threats in Oil and Gas
64	Top Threats & Controls for IoT Security	CISO Platform (2017)	IT-OT Convergence
65	Industrial Control System Threats	Dragos (2017)	IT-OT Convergence
66	Industrial Control Vulnerabilities	Dragos (2017)	IT-OT Convergence
67	Digital Transformation in Oil and Gas - Cybersecurity and Approach to Safeguard Your Business	Farooq Shaik, Arif Abdullah, S. K. (2017)	IT-OT Convergence
68	Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2)	Department of Energy - USA (2014)	Cybersecurity Policies and Guidelines

69	NCCIC/ICS-CERT Year in Review (2015)	Department of Homeland Security, NCCIC, & ICS-CERT (2015)	Cybersecurity Policies and Guidelines
70	Definitive Guide to Cybersecurity for the Oil & Gas Industry	Jason Holcomb (2016)	Cybersecurity Policies and Guidelines
71	State Roles in Enhancing the Cybersecurity of Energy Systems and Infrastructure	Andrew Kambour (2014)	Cybersecurity Policies and Guidelines
72	Cybersecurity Handbook 2017 - Resource Guide on Cybersecurity	Deepak Kumar Sahu (2017)	Cybersecurity Policies and Guidelines
73	Protecting Industrial Control Systems	ENISA (2011)	Cybersecurity Policies and Guidelines
74	Incident Reporting Framework	ENISA (2016)	Cybersecurity Policies and Guidelines
75	Report on Cybersecurity Information Sharing in the Energy Sector	ENISA (2017)	Cybersecurity Policies and Guidelines

76	Position Paper of the TNCEIP on EU Policy on Critical Energy Infrastructure Protection	European Commission (2012)	Cybersecurity Policies and Guidelines
77	EU, US go separate ways on cybersecurity	Jeremy Fleming (2013)	Cybersecurity Policies and Guidelines
78	Cybersecurity - A growing threat to the energy sector - An Australian perspective	Tim Lester (2016)	Cybersecurity Policies and Guidelines
79	National Cybersecurity Policy -2013	ISO-IEC (2012)	Cybersecurity Policies and Guidelines
80	A Comparison of Oil and Gas Segment Cybersecurity Standards	U.S. Department of Homeland Security (2004)	Cybersecurity Policies and Guidelines
81	The new CISO Leading the strategic security organization	Taryn Aguas, Khalid Kark, & Monique François (2016)	Role of Senior Management
82	The Digital Future is Now - Executive Talent Implications of Digital in Oil & Gas	Jennifer Rockwood, & Stephen C. Morse (2015)	Role of Senior Leaders

83	Identifying Cyber Risks - The Important Role of Senior Management	Tripwire (2016)	Role of Senior Management
84	Why senior leaders are the front line against cyberattacks	McKinsey & Company (2014)	Role of Senior Leaders
85	Countering the Threat of Cyberattacks in Oil and Gas	Katharina Rick et al (2016)	Role of Senior Leaders
86	Oil and gas cybersecurity - time for a seismic shift?	Allan, K., & Sutton, S. (2015)	Information Sharing and Collaboration
87	Cyber Threat Information Sharing: Recommendations for Congress and the Administration	Zheng, D. E., & Lewis, J. A. (2015)	Information Sharing and Collaboration
88	Cybersecurity and Information Sharing - Legal Challenges and Solutions	Nolan, A (2015)	Information Sharing and Collaboration
89	Oil and Natural Gas Information Sharing and Analysis Center	ONG-ISAC (2016)	Information Sharing and Collaboration

90	Information Sharing Is Key To Cybersecurity	Velda Addison (2015)	Information Sharing and Collaboration
91	Guide to Cyber Threat Information Sharing	Chris Johnson et al (2016)	Information Sharing and Collaboration
92	Science of Cyber-Security	Jason, T. M. C (2010)	Science of Cybersecurity
93	Game Theory for Cybersecurity	Shiva, S., Roy, S., & Dasgupta, D (2010)	Science of Cybersecurity
94	E-Commerce - Business, Technology	Laudon & Trever (2014)	Science of Cybersecurity
95	The Cybersecurity Management System - A Conceptual Mapping	Dexter, J. H (2002)	Science of Cybersecurity
96	Raising the Bar for Cybersecurity	Lewis, J. A (2013)	Science of Cybersecurity

7.5 Profile of the Author

C. Sundararaman

sundararamanc@hotmail.com

C. Sundararaman is a doctoral research student at the School of Business at the University of Petroleum and Energy Studies (UPES), Dehradun. He is a Chemical Engineer and completed his Master of Science from BITS, Pilani.

Sundararaman started his career at Chennai Petroleum Corporation Limited (erstwhile Madras Refineries Limited) as a Chemical Engineers. Worked in the Manufacturing segment and Training Centre for 15 years. Then he was in the field of Operator Training Simulator for 8 years. With that background he entered the IT industry. He is currently with Tech Mahindra as the Practice Head of Oil and Gas. At Tech Mahindra, he is responsible for developing digital solutions for Oil and Gas industry. He is also responsible for sales enablement, competency development and analyst relationships. Passionate in training the team members on a wide range of topics. He brings to the table an extensive understanding on the Oil and Gas value chain.

Paper publications and seminars based on this research

- **Seminars & Paper Presentation**
    - **DCMEIT2017: 2017** – Presented the paper at the 1st Doctoral Colloquium in Management Economics & Information Technology, University of Petroleum & Energy Studies, Dehradun, India, November 18, 2017. Won the best paper award.
    - **SPE Workshop: Digitalization:** Driving Data to Decisions. Presented a paper on 8th June 2018 Bengaluru, India.