CONSTITUENTS OF THE DOMAIN SPECIFIC CYBER SECURITY MANDATE FOR THE INDIAN POWER SECTOR

By

V ANANDA KUMAR

COLLEGE OF MANAGEMENT AND ECONOMICS STUDIES

DEPARTMENT OF POWER & INFRASTRUCTURE

Submitted

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

TO

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

DEHRADUN

DECEMBER, 2015

UNDER THE GUIDANCE OF

DR. KRISHAN K. PANDEY

HEAD OF DEPARTMENT – DECISION SCIENCES, CoMES, UPES, DEHRADUN

DR. DEVENDRA K. PUNIA

PROFESSOR, IET, JKLU, JAIPUR

DR. SWAMINATHAN MANI

VICE PRESIDENT, TECH MAHINDRA, HYDERABAD

To

Anvith & Ananya

ACKNOWLEDGEMENT

The journey to a PhD is seldom travelled alone. There are many who made a difference to my passage of discovery and helped me along the way, to where I stand today. I want to acknowledge the primary contribution of my guide, Dr. Krishan K. Pandey, to whom I turned to ever so often, at all times of the day and more often in the late evening and nights and whenever I faced a stumbling block. He would be calmness personified and gently navigate me around what I thought were insurmountable problems. His immense knowledge of the subject and the command over research methodology and statistical techniques paved the road and way ahead for me. To Dr. Devendra K. Punia, my co-guide with whom I have had a number of robust arguments on what I thought was superfluous addition to my research topic, to only realize that his foresight paid rich dividends down the line. The journey would not have started but for a chance meeting and a cup of coffee, with Dr. Mani Swaminathan, my friend and external guide. He was the one who convinced me to embark on this exciting expedition. His continued support all through made a big difference.

UPES blessed me with an enriching experience all through this journey of learning. The wealth of knowledge with the faculty team and more importantly their willingness to get involved, discuss, debate and provide directions is like an elixir to the seeker. Dr. Tarun Dhingra and Dr. Joji Rao would roll up their sleeves and have helped me on numerous occasions. Thanks to the Dean, Dr. Anirban Sengupta who was always approachable and a source of strength. To Dr. Bangaru Raju, Dr. Neeraj Anand, Dr. Arvind Jain and Dr. Atul Razdan who unassumingly contributed to making this an enjoyable expedition. To the team

at CCE Wg. Cdr. P.K. Gupta and then Dr. Anjali Midha and Ms. Rakhi Ruhal who were my first point of contact with UPES and a pillar of strength to the students like me.

This voyage of discovery would not have been possible, but for the support from my family, who put up with my idiosyncrasies and the endless weekends where I was not available for them, for missed vacations when I was locked up in the room and extended periods where I was completely missing. Vinu, my confidant, who spent long nights to proof read every single document that I wrote while doing my research. The only solace I had to offer to her was "that there are not too many husbands, who will willingly allow their wives to "correct" them without protest, like I do!" To my dad, who kept goading me to get my research work done at double speed, much like he would do if I were still in school. My mom, to whom I always turned to for solace.

I would fail in my duty, if I do not thank Prasenjit Saha, who introduced me to the world of security and opened my eyes to the breath-taking possibilities and opportunities in the domain. I have been fortunate to interact with many thought leaders and visionaries in the world of security, who have been ever willing to guide and help. Foremost amongst them and who I see as my role model is Dr. Paul Dorey, who while being at the pinnacle of the domain, was ever willing to guide a journeyman like me. Thank you Prasenjit and Dr. Dorey. Last, but not the least, to my colleagues and friends in Wipro from whom I learn each day. Thank you Team ESS.

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.

V. Ananda Kumar

December 2015.

THESIS COMPLETION CERTIFICATE

This is to certify that the thesis on "**Constituents of the domain specific cyber security mandate for the Indian power sector**" by **V. Ananda Kumar** 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 anywhere else for the award of any other diploma or degree of this or any other university.

External Guide

Dr. Swaminathan Mani

Internal Guide

Dr. Krishan Kumar Pandey

Co-Guide

Dr. Devendra K. Punia

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Information technology and its growth in the 20th and 21st century have had a remarkable and positive impact on society. A number of things that were in the realms of science fiction not so long ago are a reality today. The growth and the impact of the connected world, with the emergence of the Internet have outpaced anything else in the history of the human race. As we move from an era of an internet of connected people to an era of an internet of connected devices and machines, we are on the cusp of a revolution that promises to usher in a whole new reality where the real and virtual worlds merge seamlessly. This era of smart cities, smart infrastructure, smart devices and smart wearables would increase our dependency on the connected infrastructure. The connected world is not restricted just to the commercial sphere, the infrastructure which runs the nation, the nation's crown jewels and its critical infrastructure – banking, energy, telecom, transport and health among others have a huge dependency on this IT infrastructure. This IT infrastructure brings a number of advantages and benefits, but along with the upside, its own challenges.

A crippling cyber-attack on this national critical infrastructure can bring a nation down to its knees. There have been a number of well documented incidents where the critical infrastructure of nation states has been impacted by cyber-attacks. The Stuxnet, Shamoon and Anonymous incidents have shown that cyber-attacks can cause significant damage and pose a risk to National Critical Infrastructure. It is not surprising therefore, that protection of National Critical Infrastructure (NCI) against cyber threats has grabbed the attention of the world leaders. India is no exception, with cyber security topping the Indian Prime Minister, Mr. Narendra Modi's foreign policy agenda in the first 18 months of

office. Cyber-security features in 33% of his foreign policy interventions, more than any other subject.

Cyber security is a beset with the twin problems of "public-good" and information asymmetry, which results in "free-riders" and under investment, thus making cyber-security an ideal candidate for regulatory intervention. Nation states have responded by formulating cyber-security policy, guidelines and regulations to protect its NCI. Countries like the United States (US), United Kingdom (UK) and India have a documented cyber security policy and have articulated their strategy to protecting 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 focussed on the energy sector alone. The US, UK and EU have a domain specific cyber security regulation or guidelines for the power sector. North American Electric Reliability Corporation- Critical Infrastructure Protection (NERC - CIP) is an example of the power sector specific regulation.

India is poised to spend over USD 5.8 Billion as part of the National Smart Grid Mission, aimed at alleviating India's ailing power sector as part of its 12th Five year plan (2012 – 17). A significant spend in the power sector under the aegis of the R-APDRP (Restructured Accelerated Power Development and Reforms Program) is focused on building ICT capability in the utilities. There are many positives that have come about as part of the automation and IT enabled intervention. The downside is the increased threat exposure from cyber vulnerabilities. A lack of security planning, while enhancing the IT infrastructure can potentially leave gaping holes in the country's power sector stability. A key intervention would be a power sector specific cyber security mandates or policy in India which is lacking today.

This research study is focussed on understanding the cyber security challenges in the Indian Power Sector and to identity the significant constituents of the cyber security policy to enhance the security posture of the sector. The extensive literature review carried out as part of the research study was focussed on

- Understanding the impact of cyber threats to NCI, in general and to the Energy Sector in particular
- Studying the impact of cyber threats in the Indian context
- Studying the approach and regulatory intervention adopted by the US, EU and the UK to improve the security posture in the Power Sector
- Identifying the variables that form the building blocks of the cyber security policy for the Power Sector
- Identifying the theoretical constructs

The survey of the literature established the minimal literature on the cyber security challenges in the Indian Power Sector and a lack of domain specific regulations for the power sector in India. Further, the review of the theoretical constructs in cyber security showed that that there is no equivalent of the Laudon and Traver's 4 layer E-commerce security model in the cyber security domain. The research problem, objectives and questions is a continuum of the gaps in the literature.

The research study was focussed on identifying the challenges in the Indian Power Sector and identify the factors that enhance cyber security in the Indian Power Sector.

The research study was executed in two stages using "Mixed Method's research. Firstly, by leveraging Qualitative Research Strategy to identify the cyber security challenges in the power sector and subsequently to identify the factors that enhance cyber security in the power sector by using Quantitative methods.

The first three stages in the research study is captured in the figure (1) below. 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.

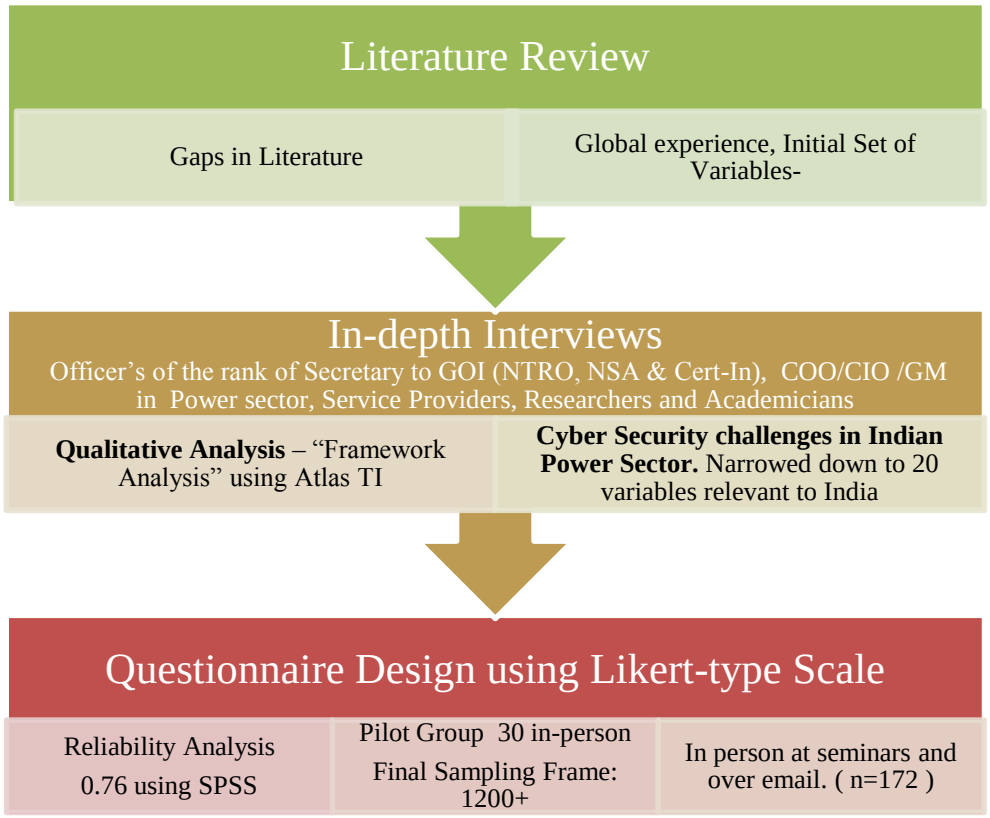

Figure 11-1: Research Design Part 1

The purposive sample of respondents for the in-depth interview were drawn from the government, industry and academia. The interviews were transcribed and analysed by adapting Ritchie 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 is captured in the succeeding paragraph.

The increased IT adoption, driven by the R-APDRP program has delivered a number of benefits with a reduction in AT&C losses across nearly all the utilities in the country. There is however, very little appreciation of the risks or exposure to cyber security threats which comes along with the increased adoption of IT both among the executives and in the rank and file of the power sector. A majority of the organization do not have designated CxO level executive responsible for cyber-security and the security function is usually subsumed within the IT organization. Given the diversity and the financial status of the players in the Indian Power Sector, a principle based regulatory intervention lead by CERC emerged as a preferred choice to enhance cyber security in the power sector. The in-depth interview also helped narrow down the focus list of 20 variables that were relevant to the Indian Power Sector. These variables were the input to the Likert-type scale for the second stage for quantitative analysis.

The questionnaire built on the 5 point Likert-type scale was administered to 172 respondents after establishing the reliability and validity. The research used Exploratory Factor Analysis to identify the initial set of six factors and then established their significance with a Confirmatory Factor Analysis as shown in Figure 2 below.

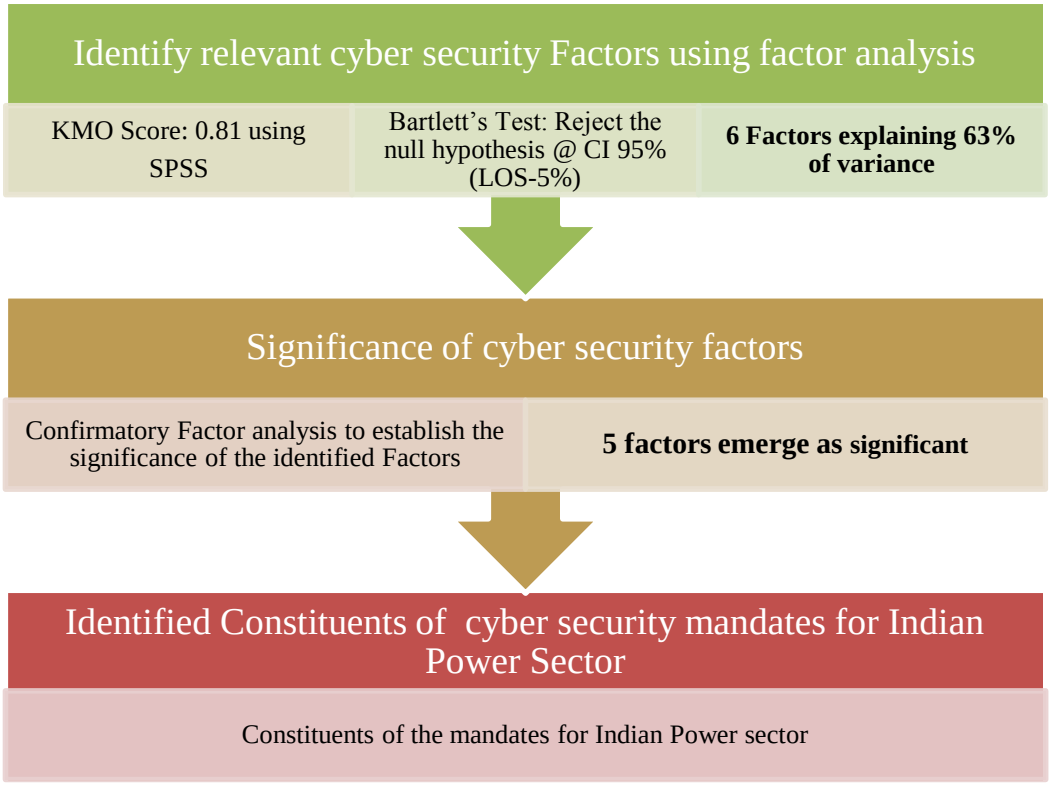

Figure 11-2: Research Design Part II

Five factors viz. Personnel & Organisation, Data Protection, Critical Cyber-Physical Asset Protection, Information Sharing & Collaboration and Security Audits emerged as significant factors from the Confirmatory Factor Analysis. These five factors are the recommended "Constituents of the domain specific cyber security mandate for the Indian Power Sector". The recommendations are explained below.

(i) Mandatory Cyber Security Guidelines for the Power Sector

The CERC should formulate the cyber security guidelines for the Indian Power Sector. The mandatory guidelines should be principle focussed,

i.e. focus on broad based standards instead of specific rules. The guideline should be outcome based and enforce senior management responsibility and accountability. The factors that enhance cyber security in the power sector and that should be included in the guidelines are covered in the subsequent recommendations.

(ii) Personnel & Organisation

A designated senior executive should be made accountable for cyber security within the organisation. Organisations should be tasked with creating a security aware culture and combined with compulsory background screening and whetting of employees.

(iii) Data Protection

The guidelines should detail the identification and protection of customer sensitive data across the entire data lifecycle including data retention requirements. Disclosure of data breach should be made mandatory with appropriate financial penalties.

(iv) Critical Cyber-Physical Asset Protection

CERC should articulate the security certifications that are required for critical cyber-physical assets in the power sector. Organisations should identify, maintain a baseline their critical cyber-physical assets. These assets should subject to periodic security reviews.

(v) Information Sharing & Collaboration (IS&C)

Organisations should be tasked to set up a critical incident response team and define the process to react to a cyber-emergency. CERC should facilitate the setup of a forum for the players in the power sector and

promote information sharing and collaboration including disclosure of cyber security incidents.

(vi) Security Audits

Organisations should be mandated to conduct self-assessments for evaluating their cyber security posture apart from periodic third party security audits. CERC should facilitate Industry wide security drills to prepare the organisations to handle a real life cyber –security incident.

Laudon and Traver propose a 4 layer cyber security model for the e-commerce sector includes Data Protection, Technology, Organisation Policies and Procedures with Laws & Industry standards forming the outermost concentric circle. All the four layers are relevant in the context of the power sector as well. However, the power sector also brings with it the nuance of protection of cyber-physical assets which does not play a role in the e-commerce world. In the power sector co-embedded with the data to be protected we would need to include critical cyber-physical assets The contribution to theory from this research is the extension of the Laudon and Traver's 4 layer e-commerce security model by including cyber-physical assets when it comes to cyber-security for the power sector.

Automation and IT proliferation in the power sector is a given, in fact is a dire need in the Indian Power Sector. The government should ensure that while it is promoting the larger adoption of IT, it does not expose an Achilles heel. Formulating and mandating the cyber security guidelines for the power sector will go a long way in addressing this requirement and enhance India's security posture.

LIST OF ABBREVIATION

Abbreviation	Expansion
AGFI	Adjusted Goodness of Fit Index
AT&C	Aggregate Technical and Commercial
CBI	Central Bureau of Investigations – India
CERT-In	Indian Computer Emergency Response Team
CESG	Communications-Electronics Security Group
CFA	Confirmatory Factor Analysis
CFI	Comparative Fit Index
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
COTS	Commercial of The Shelf products
CPA	Commercial Product Assurance
CPNI	Centre for Protection of National Infrastructure
CR	Composite Reliability
CRQ	Central Research Question
DECC	Department of Energy & Climate Change
DeITY	Department of Electronics and Information Technology
DHS	Department of Homeland Security

Abbreviation	Expansion
DMS	Distribution Management Systems
EFA	Exploratory Factor Analysis
ENISA	European Network and Information Security Agency
ERO	Electric Reliability Organization
FSLC	Federal Senior Leadership Council
GFI	Goodness of Fit Indicator
ICS	Industrial Control Systems
IDSA	Institute of Defence Studies and Analysis
IEX	Information Exchanges - UK
IP	Internet Protocol
ISAC	Information sharing and collaboration
ISACs	Information Sharing and Analysis Centers - US
KMO	Kaiser-Mayer-Olkin
MHA	Ministry of Home Affairs
MI	Modification Indices
NCI	National Critical Infrastructure
NCII	National Critical Information Infrastructure

Abbreviation	Expansion
NCIIPC	National Critical Information Infrastructure Protection Centre
NCIJTF	National Cybercrime Investigation Joint Task Force
NCP	National Cybersecurity Policy
NERC CIP	North American Electric Reliability Corporation Critical Infrastructure Protection
NIB	National Information Board
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology - US
NSA	National Security Advisor
NTRO	National Technical Research Organization
OCSIA	Office of Cyber Security & Information Assurance
OSVDB	Open-Source Vulnerabilities Database
OT	Operation Technology
PAR	Pressure And Release
R-APDRP	Restructured-Accelerated Power Development and Reforms Programme
RC3	Regional Consortium Coordinating Council
RMP	Risk Management Process
RMSEA	Root Mean Square Error of Approximation

Abbreviation	Expansion
SCADA	Supervisory Control and Data Acquisition
SCC	Sector Coordinating Councils
SCSIE	SCADA and Control Systems Information Exchange
SEB	State Electricity Board
SEM	Structure Equation Modelling
SLTTGCC	State, Local, Tribal and Territorial Government Coordinating Council
SMAC	Social, Mobile, Analytics, and Cloud
SSA	Sector Specific Agency
SSAT	SCADA Self-Assessment tool

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

1.1 OVERVIEW

This chapter highlights the need for cyber security in the national critical infrastructure and specifically in the power sector. It highlights the characteristics of cyber security that favour a regulatory intervention. It articulates the business problem and the need for the research. It concludes with the organisation of this research study.

1.2 INTRODUCTION

In today's interconnected world, Information Technology (IT) is the sub stratum that binds national critical infrastructure and the vehicle of economic progress globally. This information infrastructure has also become an attractive soft target for attacks both from within the nation and inimical forces outside. A successful attack on the nation's critical information infrastructure can bring it to a grinding halt. In the physical world there is a clear demarcation of roles and responsibility and the government with its defence forces are the primary protectors of the nation's boundaries and the police forces ensure internal security. When it comes to protecting the national critical information infrastructure however, it needs the coordination of multiple agencies and participation of the private industry to drive security making it more onerous task.

National Critical Infrastructure (NCI) has been facing cyber-attacks globally. The attacks in Baltics (Tikk, Kaska, & Vihul, 2010), Stuxnet in Iran (Brown G. D., 2011), Shamoon in Saudi Arabia (Bronk & Tikk-Ringas, 2013) and the Anonymous attacks on banks in the US have been widely covered. That the problem is wide spread is reflected as between 15 to 40% of the executives polled across APAC, Europe and USA reporting attempts at extortion with cyber threats (Zetter, Report: Critical Infrastructures Under Constant Cyberattack Globally, 2010) as shown in Figure 1 below.

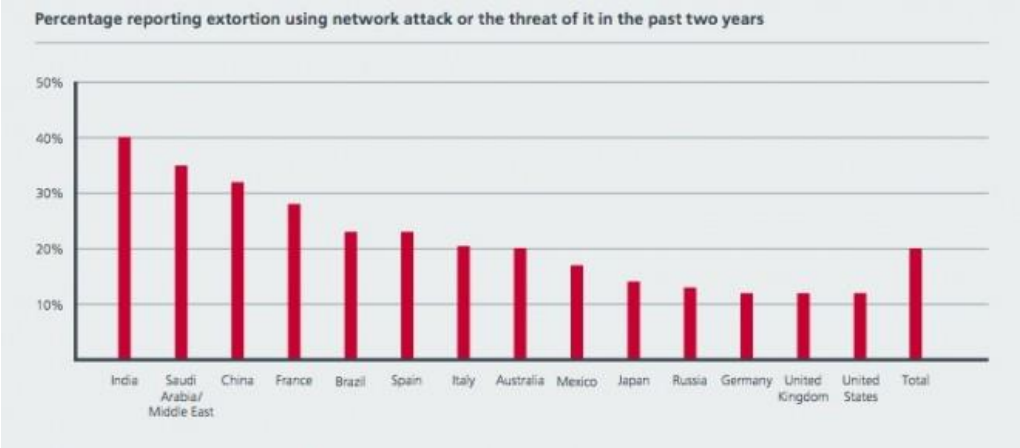

Figure 1-1: Percentage of NCI executives reporting extortion threats

The cyberspace is seen as a fifth theatre of war and many countries including the US have set up a cyber-command both as a deterrent and an offensive capability (Institute for Defense Studies and Analysis, 2012). Secure cyberspace becomes a pre-requisite for social wellbeing. Cybersecurity should thus be an integral part of India's overall national security strategy.

While the threat to national critical infrastructure spans all the domains, the energy sector bears the brunt of the cyber-attacks with close to half the attacks focused on the energy sector. With increased privatization in the Indian power sector, the ownership is dispersed amongst both the government and private sector with public having a significant stake. India is poised to spend over USD 5.8 Billion as part of the National Smart Grid Mission aimed to alleviate India's

ailing power sector as part of its 12th Five year plan (2012 – 17). The federal government sponsored R-APDRP (Restructured Accelerated Power Development and Reforms Program) is also focused on building ICT capability in the state sector. A lack of security planning as part of designing the IT infrastructure in the power sector can potentially leave gaping holes in the country's power sector stability.

Cyber security is often characterised as a "public good" and as having asymmetrical information – two characteristics that suggest the need for a regulatory intervention. Presently however, there are no power sector specific cyber security mandates or policies in India. A domain specific cybersecurity policy for the power sector that sets out the vision, objectives and approach to addressing the cybersecurity threats will help string together the individual players and ensure that the common goal of national security in ensured.

1.3 BUSINESS PROBLEM

The ICT sector plays a significant role in the economic growth and prosperity of a nation both in the developed and developing world (Vu, n.d) and India is no exception. NASSCOM, the industry body representing the IT and ITES industry estimates that the sector is a source of direct and indirect employment to over 10 million people and contributes to over USD 100 Billion in Revenue (2012 Estimates) and drives 7.5% of the national GDP (NASSCOM, n.d.). In the 5 year period from 2006 to 2011 the value of National Electronic Fund transfer (NEFT) transactions in the Indian banks grow over 12 fold to cross over INR 900,000 Crores mark. (Note: 1 Crore = 10 Million) (Lal & Saluja, 2012). The Indian Telecom industry is the second largest in the world in terms of subscriber base (Press Information Bureau, n.d.) and probably with the lowest tariff in the world. With close to 200 million users India also represents the third largest internet user population in the world (Internet world stats, 2012).

Landis+Gyr were awarded the contract to deploy over 1.5 million smart meters in the eastern state of West Bengal (Renewable Energy Technology, 2013). These are a few statistical points amongst many more that show how India's economic wellbeing is intertwined with the cybersecurity of its NCI.

The power sector is at the heart of the national critical infrastructure, an impact or downtime in the power sector will have a cascading impact on every other parts of the national infrastructure. The northern grid collapse in India during the summer of 2012, which is often called as the largest blackout in history affected over half a billion people and impacted rail transport, suburban transport, water facilities and industry (Yardley & Harris, 2012). The business problem can be summarized as: "***Deficient cyber security in the Indian Power sector threatens business growth, economy and national security".***

1.4 RATIONALE AND MOTIVATION

The Power sector is the lifeline of the nation. In today's world integral to the flow of power from generation to distribution via the transmission grid, is also the flow of information in the grid as shown in the "Electricity and Information" or the "E+I" (NIST, 2010) flow that is shown in the Figure 1-2 below. Uninterrupted and secure information and communication flow is as essential to the upkeep of the grid as the flow of the actual power supply. The increased adoption of "commercial off the shelf" for the Process Control network for automation in the power plants coupled with the complexity of the systems that is used to manage and run the grids increases the threat landscape in the power sector environment.

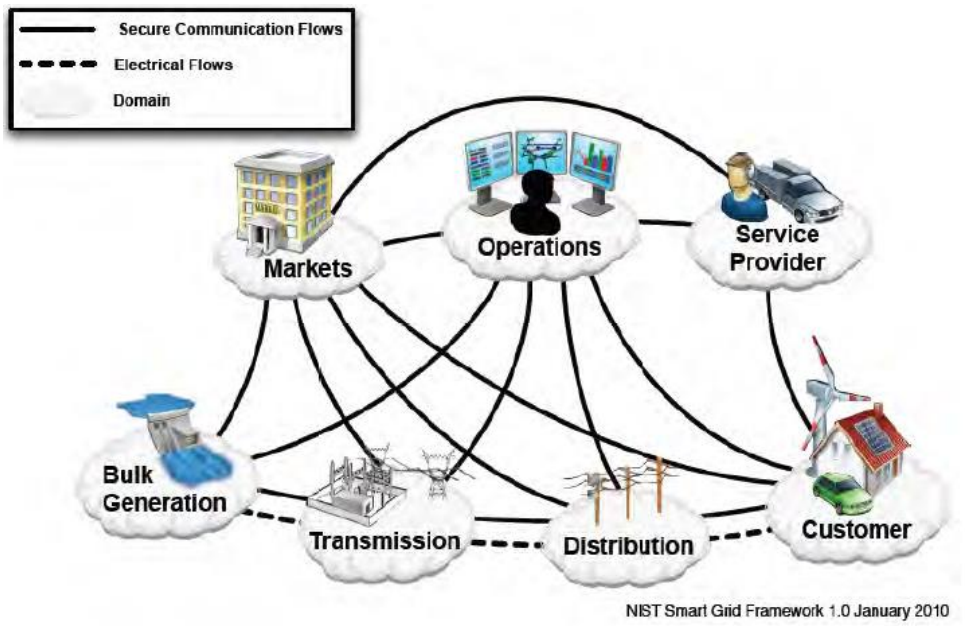

Figure 1-2: "E+I" Flow in the power sector. Source NIST Smart Grid Framework (NIST, 2010)

The attractiveness of the powe sector as a target combined with the increased threat surface for cyber attacks in the power sector, has meant that well over half the security incidents in the year 2013 were focussed on the power sector as depicted in the Figure 1-3 below (Patel, 2014).

Like in all research endeavours the review of the literature was the starting point of this study. The extensive review of the literature validated that cyber security vulnerabilities threaten the National Critical Infrastructure (NCI) globally and in India. The literature review helped establish the need for the Government regulations and mandates to improve security posture and examples of advanced nations like the US, EU and UK that have an existing or proposed domain specific regulations / guideline for the power sector. The review also highlighted the fact that cyber security is nascent domain with little theoretical underpinning and is categorized as "Use Inspired Basic" Research. The research gap helped establish the research objective or scope of the research the scope of this research study. T

he research objective of this study is to understand the cyber ecurity challenges in the Indian power sector and determine the constituents of the cyber security mandate for the Indian power sector.

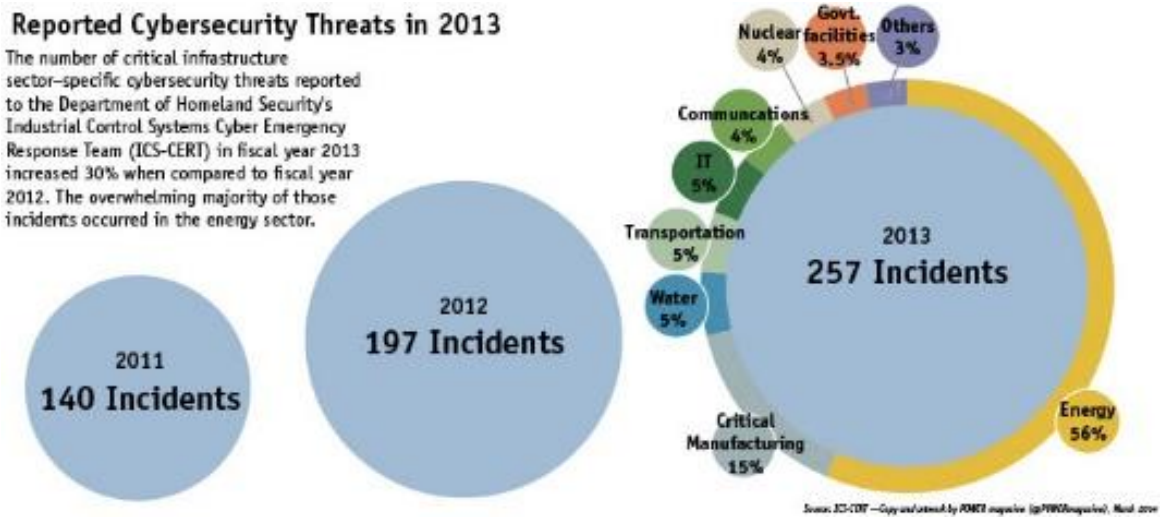

Figure 1-3: Reported Cybersecurity incidents {Source ICS-CERT cited in (Patel, 2014)}

The Research Question (RQ) for the study is to understand the current cyber security challenges in the India power sector and the Central Research Question that this study aims to answer is ***"What are the relevant factors that enhance cyber security and their significance in the Indian Power Sector?"***

1.5 OUTLINE OF THE STUDY

The research strategy of this study was aligned to meet the research objective and questions. This research was executed by leveraging Mixed Methods research. Qualitative Research strategy and the analysis of the outcome of in-

depth interview helped address the first question, and understand the cyber security challenges in the power sector.

The follow on Quantitative Research strategy was used to determine the constituents of the cyber security mandate for the Indian power sector. Exploratory Factor Analysis and Confirmatory Factor Analysis technique helped determine the factors and establish their significance.

1.6 CONTRIBUTION OF THE STUDY

The research contribution is two-fold. The research helped in identifying the cyber security challenges in the Indian power sector and followed it up by determining the factors that help enhance the cyber security posture in the Indian power sector. The research contribution to the existing body of knowledge or theoretical construct is to enhance and adapt the 4 layer Laudon and Traver security model for the power sector or potentially to other asset heavy industry.

1.7 ORGANISATION OF THE REPORT

The research study is organised in the following sections

Chapter 1: Introduction. The current chapter provides an introduction to the research study and highlights the issues and challenges in the cyber security domain. It provides a bird's eye view of the entire research.

Chapter 2: Literature Review. The Literature review summarises the existing body pf knowledge in this domain. The literature review identifies the cyber security threats to the national critical infrastructure and power sector in particular. It establishes the need for a regulatory intervention to enhance the

cyber security posture. The review highlights the domain specific cyber security regulations and mandates for the power sector in advanced countries. The literature review also establishes the research gaps and helped determine the initial set of variables that would enhance the cyber security posture.

Chapter 3: Cyber security challenges in the power sector, the need for domain specific cyber security framework in India. The chapter highlights the cyber security challenges and security threats across the entire power sector value chain – from generation, transmission and distribution. It builds the case for a domain specific cyber security regulation in the Indian power sector.

Chapter 4: Research Design. This chapter provides the blue-print for the entire research study. It calls out the research philosophy, the ontological and epistemological considerations, and the choice of research strategy with the justification of the choices made. It calls out 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 chapter on data analysis is essentially the execution of the blue-print and road map laid out in the research design. It highlights the qualitative and quantitative research techniques used to answer the research questions. It details out the approach to qualitative data analysis using Framework Analysis to analyse the in-depth interviews with the help of Atlas-TI tool. The second section of the chapter details the quantitative data analysis to answer the Central Research Question using the IBM SPSS and Amos tool sets.

Chapter 6: Conclusion and Recommendations. The final chapter calls out the recommendations for enhancing the cyber security in the Indian power sector and opportunities for future research. This is followed by the Bibliography and appendices.

Chapter 6 is followed by the Appendices including the interview protocol used, the detailed questionnaire that was used for data gathering, bibliography and the profile of the author.

1.8 CONCLUDING REMARKS

A nation's well-being and economic progress is intertwined with its critical infrastructure. In today's context and in the world of smart cities, smart devices and internet of things, critical infrastructure protection spans to the cyber world. That the cyber space is now the fifth theatre of war, beyond the traditional four theatres of land, water, air and space, succinctly summarises the importance of the cyber space and its threat surface. Unlike in the physical world, where the government or the sovereign is responsible for protecting the nation's boundaries, in the cyber world the ownership and therefore the responsibility spread spans the government sector, private sector and the individual citizen. The nation's cyber security policy is the apex document that weaves together the individual responsibilities to form a cohesive and strong defence. The power sector is the heart beat and enables the functioning of the remaining critical infrastructure sectors and is also the one that faces the disproportionate majority of the attacks. The Indian power sector, while it is plagued with a number of challenges, has been investing in automation and expanding its information technology foot-print. While IT enablement and automation are a much needed investment, baking in security requirements is a key requirement for its continued success. A domain specific cyber security policy will serve to enhance the security posture of the organisations in this sector. The research identifies the challenges in the Indian power sector and the factors that would enhance the cyber posture of the organisations in the power sector. It is hoped that this research will contribute in a small way to building a cyber-safe nation.

2 LITERATURE REVIEW

2.1 OVERVIEW

The aim of the literature review is to understand the existing body of knowledge in a domain and is the "point of departure" of the research journey. This literature review covers the impact of cyber threats to National Critical Infrastructure (NCI) across the globe and in India, with specific emphasis on the power sector. The review discusses the policy / regulatory intervention adapted by the United States, European Union and United Kingdom to improve the security posture of their national critical infrastructure in general and the power sector in particular. The review also seeks to study the theoretical constructs in the cyber security domain and finally to identify the gaps in the literature that would become the basis for the research problem.

2.2 INTRODUCTION

The Literature review is the starting point of any research and is an attempt to understand the existing body of knowledge in the domain of interest. The objectives of a literature review as Hart points out are { (Hart, 1998) as cited by (Randolph, 2009)}:

- Distinguishing what has been done from what needs to be done,
- Identifying variables relevant to the topic,
- Synthesizing and gaining a new perspective,
- Establishing the context of the problem

Cooper's (Cooper, 1988) Taxonomy of Literature Review provides the framework to plan and approach a literature review. Cooper recommends that the literature review be classified according to five characteristics and their sub-levels viz.:

- Focus: Research outcome, Research methods, Theories, Practice or applications
- Goal: Integration, Criticism, Identification of central issues
- Perspective: Neutral representation or Espousal of a cause
- Coverage: Exhaustive, Exhaustive with selective citation, Representative, Central or Pivotal
- Organization: Historical, Conceptual, Methodological
- Audience: Specialized scholars, General scholars, Practitioners or policy makers, General public

In the table 2-1 below, the characteristic, choice of level and approach taken in this literature review are summarized. The focus areas of this literature review include:

- To study the impact of cyber vulnerabilities and threats to the National Critical Infrastructure across the globe
- To study the impact of cyber vulnerabilities and threats to the Energy sector
- To understand the impact of cyber threats to the National Critical Infrastructure in India
- To study the approach and regulatory intervention adopted by US and UK to improve the security posture of National Critical Infrastructure in general and in the power sector specifically
- To identify the list of variables that form the core building block of the cyber security policy for the power sector in a country

- To study the theoretical constructs in the cyber security domain
- To identify the gaps in the literature / research

Characteristics	*Choice of Primary Category for this literature review based on Cooper's Taxonomy*
Focus	Research Outcomes
Goal	Integration and Identification of central issues
Perspective	Neutral representation
Coverage	Exhaustive with selective citation
Organization	Conceptual

Table 2-1: Cooper's Taxonomy of Literature Reviews ((Cooper, 1988) as cited by (Randolph, 2009))

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, NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) and research work carried out by think tanks and industrial bodies like Institute of Defence Strategy and Analysis (IDSA) and Data Security Council of India (DSCI) amongst others. We focus on the experience in the United States of America (US) and the United Kingdom (U. K) as the US has been the pioneer in the domain of cyber security and India shares a similar judicial and bureaucratic structure with the United Kingdom.

2.3 NATIONAL CRITICAL INFRASTRUCTURE (NCI): DEFINITION

The Oxford dictionary defines "Infrastructure" as the basic physical and organizational structures and facilities (e.g. buildings, roads, power supplies) needed for the operation of a society or an enterprise. The United States'

Presidential Decision Directives – 63 (PDD – 63), published in 1998 under the aegis of President Bill Clinton, is perceived as a seminal policy document (McGowan, 2013) that laid out the need for Critical Infrastructure protection and the nation's policy response. PDD-63, defines Critical infrastructures as those physical and cyber-based systems essential to the minimum operations of the economy and government (Department of Commerce, US Government Publishing Office, 1998). The Directive identified sixteen sectors as critical to the wellbeing of the nation. These sectors range from telecommunication, energy, banking and finance, transportation and emergency services amongst others and is spread across both the government and private domains. In the US, The Department of Homeland Security (DHS) is the nodal agency for protection of Critical Infrastructure. The DHS identifies and calls out cyberspace as the "nervous system" and the "control system" of the nation (Department of Homeland Security, 2003) and US National Strategy to Secure Cyberspace lays out the government approach to addressing the cyber security risk.

The United Kingdom (UK) follows a similar approach and defines national infrastructure as "those facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends" (Cabinet Office, United Kingdom, 2010). The Centre for Protection of National Infrastructure (CPNI) lists nine sectors that form part of National Infrastructure in UK. In the UK the Cabinet office is the nodal agency responsible for Cybersecurity. The UK identifies cyber as a Tier One risk as part of its National Security Strategy (UK Government, 2010) and calls out cyberattacks by other nation states, terrorists or organized crime as a priority.

There is limited literature on definition of Critical Infrastructure in India or identification of sectors that are categorized as National Critical Infrastructure. The Information Technology Act 2000, however provides a definition of Critical Information Infrastructure as "computer resources, the incapacitation or

destruction of which, shall have debilitating impact on national security, economy, public health or safety" (National Technical Research Organisation, 2013). The Department of Electronics and Information Technology (DeITY), as part of its Critical Information Infrastructure policy document calls out Defence, Finance, Energy, Transportation and Telecommunication as part of critical infrastructure in India (Department of Electronics and Information Technology, n.d.).

2.3.1 CYBER SECURITY VULNERABILITIES THREATENS THE NATIONAL CRITICAL INFRASTRUCTURE

Marc Goodman succinctly 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.

In today's world National Critical Infrastructure (NCI) is an integration of smaller systems into larger systems facilitated by modern information communication and technology. 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. This combined with poor security awareness and lack of penalties or costs to private actions when there is a system disruption has served to increase the vulnerabilities in National Critical Infrastructure (Kroger, 2008). While innovation brings with it significant benefits, Tomas Hellstorm (Hellstorm, 2007) in his work brings out how disruptive innovations also serves to increase the vulnerabilities in the NCI. He identifies three types of effects that causes vulnerabilities in NCI

- Direct infrastructure effects
- Indirect infrastructure effects
- Exploitation of infrastructure

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.

Industrial Control Systems (ICS) monitor and control complex industrial processes like petroleum refinement, chemical production, product manufacturing, and electric power generation and transmission. Modern ICS infrastructures consist of a variety of intelligent, microprocessor-based equipment communicating over potentially complex distributed network links (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).

This is significant because the 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 damage that can be caused by a successful attack on the SCADA systems to NCI (Nicholson, Webber, Dyer, Patel, & Janicke, 2012). There is sufficient literature to establish that NCI is susceptible to cyber security attacks and modern day "smart" infrastructure serves to provide a larger threat landscape that increases the vulnerabilities.

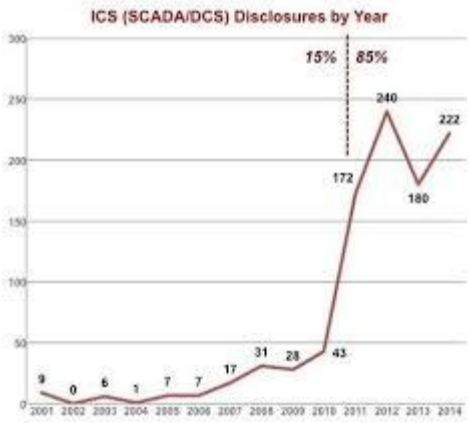

Figure 2-1: ICS Disclosures 2001 to 2014 (Source: (Knapp & Langill, 2015))

2.3.2 ENERGY SECTOR BEARS THE BRUNT OF CYBER-ATTACKS

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, Dyer, Patel, & Janicke, 2012). This assessment is shared and corroborated by other researchers as well, who have come to similar conclusions.

Candid Wueest in the Symantec research report concludes that the "energy sector has become a major focus for targeted attacks" (Wueest, 2014).

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).

This pattern of targeted cyber-attacks focused on the energy sector has remained a consistent phenomenon in the recent years as shown in the pie charts in Figure 2-2 and Figure 2-3 below. The analysis of the data in the two figures below

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.

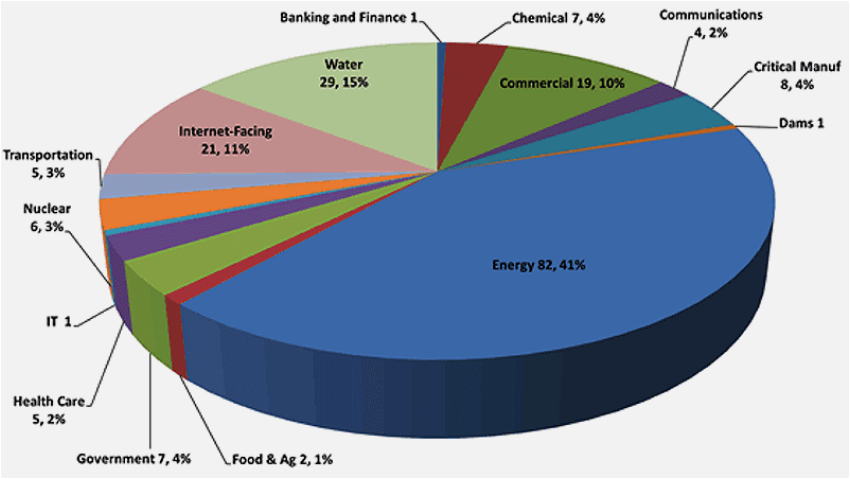

Figure 2-2: Year: 2012. 40% of the cyber-attacks on the critical infrastructure were targeted at the Energy Sector {Source ICS CERT as cited in (N-Dimension Solutions Inc, 2015)}

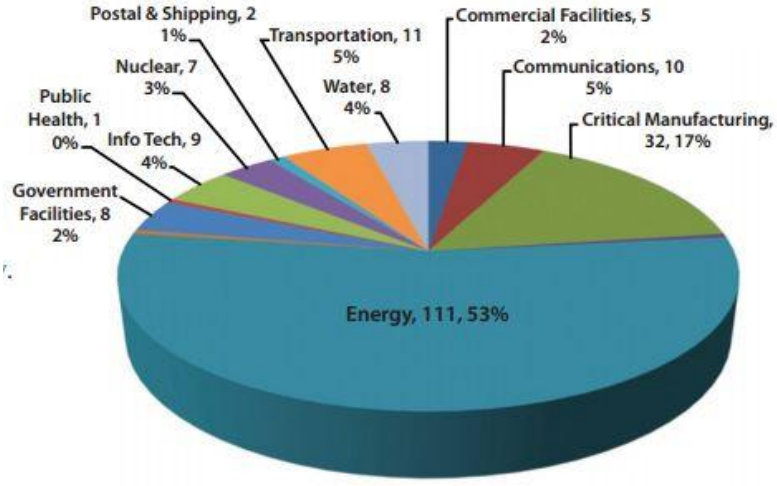

Figure 2-3: 2012-13. 53% of the Cyber-attacks on the critical infrastructure was targeted at the Energy Sector {Source ICS Cert as cited in (Paganini, 2013)}

2.4 CYBER THREATS IN THE POWER SECTOR

Cyber security threats in the power sector can be broadly classified based on the source of the vulnerabilities into three areas listed below:

- Generic threats attributed to the vulnerability in the Industrial Control Systems (ICS) or operational systems: This includes the threats that seek to exploit the generic vulnerabilities in the Supervisory Control And Data Acquisition (SCADA) systems or Distribution Control Systems (DCS). These control systems, when used in the power sector could put the power sector at risk.
- Threats specifically targeting the vulnerabilities in the Smart Grid: This includes the threats that seek to exploit the vulnerabilities as the power sector witnesses a larger global adoption of Smart-grids that replaces the analog devices to IP based smart devices.
- Generic threats attributed to the vulnerability in the IT systems: This includes the threats that seek to exploit the vulnerabilities in the IT systems that are part of the enterprise or the business network of the power sector. While these are vulnerabilities are common to the operating systems or database or network devices etc., they can be exploited to impact the power sector.

2.4.1 VULNERABILITIES IN THE SCADA SYSTEMS AND DCS SYSTEMS

Exploits of vulnerabilities in control system is a recent phenomenon as discussed earlier. The July 2010 discovery of the Stuxnet malware represented a paradigm shift in the history of cyber security and cyber warfare (Lee, 2011). The Stuxnet malware was combination of the first ever Programmable Logical Control (PLC) rootkit, a zero day exploit of Microsoft Windows, stolen digital certificates and the integration with a command and control and a peer to peer

update capability. Robert Lee calls it the most advanced malware ever to be released. It is often compared to the "cruise missile" (Barnes, 2010) in its ability to seek out and destroy a specific target – in this case the nuclear facility in Iran. All this lead to the speculation that Stuxnet was an instrument of state sponsored cyber-attack (Langer, 2011). This incident changed the discourse on cyber security and cyber warfare as it demonstrated how even large governments were vulnerable to a cyber-attack and yet the attack can remain undetected for a long time (Lee, 2011). Gregory Hale (Hale, 2011) and (Zetter, Scada Exploits, 2012) point out additional exploits in the control systems that can have a significant impact on Power sector. Ryu et al., in their research highlight the cause of vulnerabilities present in SCADA systems and security threat that emanates from the vulnerabilities (Ryu, Kim, & Um, 2009). Ralston et al.'s works focus on the key areas of concern for SCADA and DCS systems and they provide an approach to risk assessments for SCADA and ICS. Ryu et al (Ryu, Kim, & Um, 2009), and Kim Zetter's work in a similar vein, points out the numerous vulnerabilities in the SCADA system and how SCADA exploits impacts NCI (Zetter, Scada Exploits, 2012).

2.4.2 VULNERABILITIES IN THE SMART GRID

The second type of threats in the power sector are the potential exploits of the power system components – from the generation station, to transmission lines and distribution systems. As the power sector sees an increase in the adoption of the smart grids and smart metering that increases the threat surface. The Smart grid's pose a difficult cyber security challenge as it is different from traditional IT networks (Falk & Fries, 2011). The unique characteristics of the smart grid include:

- The long life time of asset, which means that the system would need to work with legacy infrastructure
- Constrained resources for field devices and Remote Terminal Units (RTU)

- Asymmetric and real time communication requirements
- High availability and low latency requirements
- Challenges with the physical security of devices

Paul, Shuva et al, in their paper point out that he key objectives of a security program in a smart grid is to prevent the reputational loss, denial of service, violation of the privacy of their customers, the hijacking control of equipment and services or cause automated systems to waste resources on false alarms (Paul, Das Gupta, Islam, Saha, & Majumder, 2012). Wang & Lu, in their survey of smart grid security challenges focus on the communication network architecture in the smart grid and the underlying SCADA protocols that support the communication layer (Wang & Lu, 2013). They point out that in the security triad of Availability, Integrity and Confidentiality, Availability is the key component in power systems and is more important than Confidentiality. The author's classify the attack patterns into 3 vectors:

- Attacks affecting the availability (or Denial of Service)
- Attacks on the confidentiality and
- Attacks on the integrity of the system

The authors discuss the various models of risk assessment including Probability risk assessments (PRA), Graphic based risk assessment, and security metric based assessment as an input to the planning process.

Pearson identifies the five most pressing challenges in a smart grid (Pearson, 2011). They are the large amount of customer sensitive information that needs to be managed, a large of sensor devices in the network, poor physical security of these devices, the move away from industry specific communication hardware / software and the greater number of stakeholders that will need to interact for smooth operations. The integration of advanced computing with power systems introduces serious cyber security concerns and this is accentuated in the smart grids (Zhaoyang, 2014).

Michael Gross' (Gross, 2011) work, builds on the Stuxnet incident and the threats to the generation plants from such attacks. Clemente (Clemente, 2009) in his research work balances the benefits of the smart grid against the threat vectors. The paper points out that the critical infrastructure is vulnerable to cyber threats and focuses on the vulnerabilities in the Transmission network. The author suggests a risk based approach to addressing the security vulnerabilities. Deng and Shukla's work substantiates the key cyber security risks in the transmission infrastructure of the power grid (Deng & Shukla, 2012). Their paper discusses how the effect of traditional cyber security attacks like "Man in the Middle" and Distributed Denial of Service affect the transmission subsystem. In a similar vein, Anderson and Fuloria, in their review paper, discuss the various cyber security threats in the Advanced Metering Infrastructure (AMI) infrastructure and how it affects the distribution system and the power grid cyber security (Anderson & Fuloria, Smart meter security: A survey, 2011).

The existing body of knowledge establishes the cyber security impact across the entire power system value chain – from generation, distribution and transmission in the smart grid.

2.4.3 VULNERABILITIES IN THE IT SYSTEMS OF THE POWER SECTOR

The third area of exposure to cyber threats are from the vulnerabilities in the IT systems in the power plant. The vulnerabilities and exploits of the IT system have been documented quite often. Alan Brown describes how cyber security professionals were able to get access to core corporate systems, map the entire OT systems and access critical information in matter of minutes by exploiting known IT vulnerabilities in a power plant (Brown A. , 2002). David Watts highlights a number of vulnerabilities in the IT domain which can be exploited and impact the power systems. These include improper security configuration in Operating Systems (OS), network devices and, wireless systems. He points

out that over 90% of the successful attacks make use of known security vulnerabilities in OS or network devices (Watts, 2003).

Apart from the conventional IT systems found in all enterprises, power plants need to deal with Operations Technology or OT. Gartner defines OT as the hardware and software that detects or causes a change through monitoring and control of physical devices, processes and events in an enterprise (Gartner Inc, n.d). The traditional approach to security the power plants is to ensure that there is an "Air Gap" between the corporate systems or information technology (IT) systems and power systems or the Operational Technology (OT). This lulls the team into believing that vulnerabilities in the IT world would not impact the OT world. Eric Byres breaks this myth and argues that attempting to use isolation as a security strategy for critical systems is unrealistic in an increasingly connected world (Byres, 2013).

Fovino Nai et al. breakdown the ICT network in a power plant into its component systems - Field network, Process network, Process firewalls, Data network and Company intranet and discuss issues at each of the component parts. They narrow down to the key vulnerabilities to architectural vulnerabilities, weak separation of networks, lack of authentication in the protocols, multiple single point of failures, security policy vulnerabilities and software vulnerabilities. They point out that security threats can be caused any number of groups - hackers, insiders, organized crime, terrorists and nation states.

The review of the literature brings out the threats faced by the power sector from cyber security exploits and vulnerabilities.

2.5 CYBER THREATS TO THE NATIONAL CRITICAL INFRASTRUCTURE (NCI) IN INDIA

As with any other nation, India too faces threats from forces that are inimical to its interests. In the modern era, these threats also expand to the cyber domain. However, there is very limited peer reviewed literature that details out the cyber security incidents on critical infrastructure in India. The most authentic source of data on the cyber security incidents in India comes from the Indian Computer Emergency Response Team (CERT-In) that provides details of the security incidents in India as part of its Annual report.

Indian Computer Emergency Response Team (CERT-In) reported a 236 fold increase in cyber security incidents in 8 years leading to 2014. In the year 2006, when the report was published for the first time, CERT-In reported 536 security incidents (Indian Computer Emergency Response Team (CERT-In), 2007) and in their latest annual report in 2014, they recorded over 130,000+ incidents (Indian Computer Emergency Response Team (Cert-In), 2015). The dramatic increase in volume of incidents was compounded by the increased severity of the incidents over the years. In 2006, the vast majority of the incidents involved Phishing and Network Scans, whereas in 2014 the major incidents included malware which targeted payment kiosks in the transit systems and malware targeting the SCADA and Industrial Control Systems.

The Union Minister for Communication and Information Technology, Ravi Shankar Prasad in his statement in the National Parliament placed on record that India faced hacking and other computer attacks from individuals or organizations in Pakistan, China, United States and Bangladesh (Press Trust of India, 2015).

Institute of Defence Studies and Analysis (IDSA) in their report titled India's Cyber Security Challenge, highlights the key threats facing India and India's

National Critical Infrastructure. The report paints the "dooms day" scenario when there is combined physical and cyber-attack on India crippling the nation. They go on to make recommendation for improving India's cyber security posture (Institute for Defense Studies and Analysis, 2012).

Shadows in the Cloud: Investigating Cyber Espionage 2.0 provided a detailed investigative analysis of the how the Indian computer infrastructure was systematically targeted and compromised business and government departments in India leading to theft of sensitive documents by individuals linked to the Chinese hacking community. The victims included Defence establishments, military personnel, research bodies, Diplomatic missions and corporates (Information Warfare Monitor and Shadowserver Foundation, 2010).

Sameer Patil, (Patil, 2014) highlights that a vast majority of the Critical infrastructure systems in India, across transportation, critical manufacturing and energy sector is plagued by outdated control systems and technology infrastructure that makes it susceptible to cyber-attacks on the Supervisory Control and Data Acquisition systems, which manage their operations. He points out that a successful cyber-attack on these systems can have a devastating impact on the nation and the imperative for India to take counter-measures.

Security Research firms Symantec and Kaspersky, raised the alarm on the malware Regin, which targeted the Telecom sector in India and other countries. They go on to point out that the sophistication of the malware agent suggests that it was backed by a nation state (Press Trust of India, 2014).

The Central Electricity Authority, identified cyber security as a key threat to the national power infrastructure in India and stresses the need for implementing cyber regulations in India and arriving at a unified framework for cyber security (Government of India, Central Electricity Authority (CEA), 2013).

The Government of India recognizing the threats to its National Critical Infrastructure has published the cyber security policy and points out the need for regulation, information sharing, need for creating the required knowledge

workers in cyber security and industry, academia, government collaboration (Government of India, Ministry of Communications and IT, Department of Electronics and Information Technology, 2013).

2.6 REGULATORY MANDATES ARE KEY TO IMPROVING CYBER SECURITY

In the physical world, the role of the nation or the state in protecting its sovereignty is well established. The organs of the state, whether it is the armed forces for protecting against external threats or the police for internal threats and their role are substantially owned and governed by the government. In the cyberspace however, it is more and more likely that vast portions of the infrastructure are privately owned or managed. The government therefore on its own will not be in a position to protect the entire cyber space and neither will the private player working on its own be able to stand up to an aggressor who is backed by a nation state.

Paul Rosenzweig in his essay argues that Cyber security has dual characteristics – (a) that of a public good and (b) private good with externalities (Rosenzweig, 2011). This view is endorsed by a number of other researchers like Mischa Hansel (Hansel, 2013) and Bruce Kobayashi (Kobayashi, 2011). Public goods are beset with the problem of

- Free riders: or individuals not contributing to the creation of public goods but hoping to gain from the investment of others
- Assurance: when individuals do not contribute to the creation of public goods because they believe that there will never be sufficient cooperation and investment will be futile

The authors postulate that public nature of cyber security can result in under investment in cyber security and incentivize the “free rider” behaviour. The

Information Sharing and Analysis Centres (ISACs) in the US and Information Exchanges (IEX) in the UK for sharing of cyber security threats and incidents are based on this principle.

Elinor Ostorm differs with the view that cyber-security is a public good. She suggests that Cyber Security is "imperfect commons" or a "common pool of resources" and not a public good. However, Elinor goes on to argue that self - governance would be weak in the cyber domain because of the disparity and size of the resources, the large number of users and the poor predictability (Nye, 2010). The common ground among the various authors is the need for regulatory intervention.

James Lewis makes a forceful argument for a greater role of government in managing the internet policy. Traditionally there has been a minimal role for the government driving the policy and regulating the internet. However, Lewis argues that the private industry and commercial interests cannot stand up to a cyber-attack which is funded by the governments on the other side and it cannot be left to the industry to drive self-regulation. He quotes the examples of railways, automobiles and air travel where the government regulations were brought in to promote the sector. He contends that in the new phase of administering and securing the internet, the role of the governments would be primary (Lewis, Soverignty and the Role of Government in Cyberspace, 2010). In his subsequent research work, Lewis traces US government approach to cyber security regulations since the Marsh plan and Presidential Decision Directive 63 (PDD-63) in 1998. He casts doubt on the voluntary compliance approach and argues for Federal oversight and regulation of identified critical Infrastructure (Lewis, Raising the Bar for Cybersecurity, 2013).

Researchers like Ross Anderson and Tyler Moore who have worked extensively on the Economics of cyber security also arrive at the same conclusion of the need for regulatory intervention in cyber security. Tyler points out that Information Asymmetries and Economic barriers (Moore, 2010) in cyber security makes it an imperfect market. Ross Anderson et al., argue that there is

no incentive for the software vendor to improve the security of the software as the customers are not willing to pay a premium for increased security of the software as it is a quality that they are not able to measure (Anderson, Moore, Nagaraja, & Ozment, 2007).

Thus researchers who have approached the cyber security issue from different perspectives conclusively agree that cyber security cannot be left to the market forces and there is a need for regulatory intervention to improve cyber security posture.

2.7 POWER SECTOR CYBER SECURITY REGULATIONS IN THE US AND EU

United States and the European Union have regulatory requirements or mandates aimed at improving the cyber security of the critical Infrastructure and this is complemented by sector specific guidelines or regulations for the power sector.

2.7.1 REGULATORY INTERVENTION IN THE US

The US has been the pioneer in recognizing the risks posed cyber threats to the critical infrastructure and has both has had multiple versions of the Cybersecurity policy documents over time. The US Presidential Policy Directive -- Critical Infrastructure Security and Resilience (PPD-21) (The White House, 2013) and Executive Order 13636 - - Improving Critical Infrastructure Cybersecurity (The White House, 2013) are the most current intervention. Apart from the general security guidelines applicable across the critical infrastructure, the US has also been the pioneer in the sector specific regulatory intervention for the Energy sector. The NERC CIP or the North American Electric Reliability Corporation Critical Infrastructure Protection is the flagship program that governs the bulk electric system.

The NERC CIP has 9 standards and 45 requirements that address the entire gamut of cyber security form security of electronic perimeter, protection of critical cyber assets, personnel, security management and disaster recovery planning. In the year 2007, NERC was designated as the Electric Reliability Organization (ERO) under the Energy Policy Act, 2005 (North Amercian Electricity Reliabiity Corporation , n.d.). NERC's Reliability Standards CIP 001 through 009, which address the security of cyber assets essential to the reliable operation of the electric grid became mandatory requirements. The NERC CIP standards are the only mandatory cybersecurity standards in place across the critical infrastructures of the United States apart from those promulgated by Nuclear Regulatory commission. The CIPs have continued to evolve and expand over time, from the version 1 that was approved in 2008 to Version 5 of the critical infrastructure protection (CIP Version 5) that was approved in 2013 (North America Electric Reliability Corporation, n.d.).

The NERC-CIP covers the bulk power system and excludes the local network and the distribution network that have typically been under the jurisdiction of the states and not with the federal government. While there are suggestions that the U.S. Federal government could take action to expand coverage to the state networks as well (Malashenko, Villarreal, & Erickson, 2012), the Public Utilities Commissions in the states serves to address this requirement in the United States (Pennyslavania Public Utility Commission, 2013). A number of states, New York, Arkansas, Texas among others have adopted cyber security mandates or regulations to promote security in the networks in their jurisdiction (McCabe, 2014). The NERC CIP remains the most comprehensive regulatory intervention specific to the power sector across the US and EU. The NERC CIP and related regulations are also enhanced by the guidelines and frameworks that are published by industry bodies and standards institutes. The Executive Order 13636 on Improving Critical Infrastructure Cyber security (The White House, 2013), mandated the National Institute of Standards and Technology (NIST) to develop a voluntary framework to mitigate cyber security risks. The NIST Special Publication. SP 800-39 focusses on "Managing Information Security

Risk: Organization, Mission, and Information System View". The SP 800-39 has been adapted by the electricity subsector and it has been tailored to address the domain specific unique attributes. This tailored approach is presented as Electricity Subsector Cybersecurity Risk Management Process ("RMP") by the Department of Energy. The RMP includes the cybersecurity risk management framework and organizational structure (Smart grid Interoperability Panel, 2014). The NIST' s Smart Grid Cyber Security guidelines NISTIR 7628 and its revision is an analytical framework that organizations can use to develop effective cyber security for their specific characteristics, risks and vulnerabilities (Smart Grid Interoperability Panel, 2010).

2.7.2 REGULATORY INTERVENTION IN THE EUROPEAN UNION

The European Union takes divergent approach to Cyber security regulations as compared to the United States of America (Euractiv, 2013). The US has favoured a more voluntary reporting mechanism, while EU approach has been biased towards a compulsory compliance and reporting regime. The EU proposals and directives on Cyber security include:

- Policy on Critical Information Infrastructure Protection (CIIP)
- Commission proposal for a Directive on Network and Information Security

The objective of the CIIP is protection of Europe from cyber disruptions ad enhance the resilience and security of the key Information and Communication infrastructure. The CIIP aims to provide the stimulus to the development of security and resilience capabilities, both at national and at EU level (Europeon Commission, 2009).

The European Union proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union (European Commission , 2013). The E. U. Directive includes measures to ensure a high common level of network

and information security across the Union. The objective is to ensure that there is a structure for cooperation between nation states, framework and guidelines for the operators of critical infrastructure, including Energy companies to manage security risks and reporting of critical incidents within the state.

Apart from the proposed Directives, the EU and ENISA have issued a number of guidelines and policy suggestions for Critical Infrastructure Protection

- Incident Reporting and Security Guidelines:

  Article 13a of the EU Regulatory Framework for electronic communications requires operators to take technical and organizational measures to address cyber security risks and to report security incidents to the competent National Regulatory Authority (NRA). It provides guideline on Technical Security Measures and on Incident Reporting (ENISA, n.d.).

- Protecting Industrial Control Systems: Recommendation for Europe and Member States:

  The report delves into threats, risks and challenges in the area of ICS protection and provides recommendations to mitigate the risks from Industrial Control Systems (ENISA, 2011).

- ENISA Smart grid Security Recommendations

  The report identifies the key security of smart grids and makes 10 recommendations aimed at providing advice and a good practices guide to improve the security posture (ENISA, 2012).

The EU directives on cyber security are complemented by the national security guidelines or mandates that are specific to each country. The apex cyber security policy is articulated in the UK Cyber Security Strategy Protecting and promoting the UK in a digital world (Office of Cyber Security and Information Assurance in the Cabinet Office, 2011).

2.7.3 REGULATORY INTERVENTION IN THE UNITED KINGDOM

The United Kingdom (UK) has favoured a regulatory light approach to cyber security. The UK government promotes Cyber Essentials. Cyber Essentials encourages organizations to follow good practices in information security. The Cyber Essentials programme is an assurance framework aligned to the ISO 27001. It was launched in 2014 by the Department for Business, Innovation and Skills.

The Office of the gas and electricity markets (Ofgem) is the independent national regulatory authority in the UK. Ofgem governs the supply licensing agreements and is empowered to modify or amend the licenses or codes. Ofgem' s Low Carbon Network (LCN) Fund promotes the use of new technology to ensure security of supply with value for money. The security requirements of the grid are implicit in the overarching objective of contributing to energy security (Tritschler & Mackay, 2011). The Centre for Protection of National Infrastructure (CPNI) supports the UK government push to improve cyber security by publishing good practices guide and providing benchmarking services. The CPNI hosts the SCADA and Control Systems Information Exchange (SCSIE) that promotes information sharing and collaboration between companies operating in the critical infrastructure including power companies and utilities. The SCADA Self-Assessment tool (SSAT) published by CPNI helps organizations benchmark the security assurance program (Tritschler & Mackay, 2011).

The Smart metering implementation program is the central program for roll out both electricity and gas meters across Great Britain. The prospectus of the program establishes the basic Security guidelines for smart meters. The UK has defined the security requirements as part of the smart grid and smart metering roll outs lead by the Department of Energy & Climate Change (DECC). The DECC has defined

- Security Requirements and an end-to-end security architecture for Smart grids.
- Mandatory Commercial Product Assurance (CPA) certification includes security guidelines for all smart metering products in the UK.
- CESG (Communications-Electronics Security Group) provides smart metering security profiles or the "smart metering security characteristics".

There are a number of research articles that compares and contrasts the US and EU approach to cyber security regulation. Bruce May et al., highlight the Jeffrey Seifert Rule system continuum from the anarchical informal rule systems at one end and formal rule system of "world government" at the other end, with national laws and private regimes between these two. The paper studies various issues in the internet and variance in approach to address these issues by US and EU. In the US the focus is self-regulation, industry codes and consumer choice while in EU the focus is state regulation and national identity. The regulations in European Union (EU) and United states are contrasted by

- Liberal model vs. Libertarian model (minimal state intervention),
- Public service vs. Public interest
- National-cultural vs. Liberal Market

On the same lines Janine and Russell contrasts the US and European policy and legislative action to cyber security and point out that US models itself on self-regulation while the European Union (EU) favours mandatory standards.

2.8 CYBER SECURITY: THEORETICAL CONSTRUCTS

The theoretical framework or the "Science of Security" has been a particularly vexing problem. AFCEA International cyber committee that delved into the Science of Security, in their report highlight the challenges in the cyber security

domain. They point out that "Science" can either be deductive or inductive. Deductive reasoning or arriving at a generalized conclusion based on past observation is a challenge in the cyber domain, just as arriving at a conclusion based on experimental observation or Inductive reasoning. They go on to highlight that the term cyber security itself is not well defined (Brown, Klopp, Palmer, & Wolf, 2014).

One of the most comprehensive work on the subject was done by the JASON project. The report higlights the challenge in building a theoretical construct. Cyber-security being an artificial construct has meant that there are very few a priori constraints on either the attackers or the defenders. This challenge is further compounded by the dynamic nature of the threats associated with cyber-security the response. Thus there is no one area of science (mathematical, physical, or social) that would comprehensively address all the salient issues (JASON, The Mitre Corporation, 2010). The report recommends the establishment of interdisciplinary centers that brings together academia, industry and national laboratories. The research cite's Stoke's tripartite division of research. The classification is based on whether the research advances human knowledge by seeking a fundamental understanding or motivated by the need to solve immediate problems { (Stokes, 1997) as cited in (JASON, The Mitre Corporation, 2010)}. Based on this model Research be classified into one of the three buckets as shown in the Figure 2-4 below.

- Pure basic research (or the Bohr Quadrant).
- Pure applied research (or the Edison Quadrant).
- Use-inspired basic research (or the "Pasteur's Quadrant").

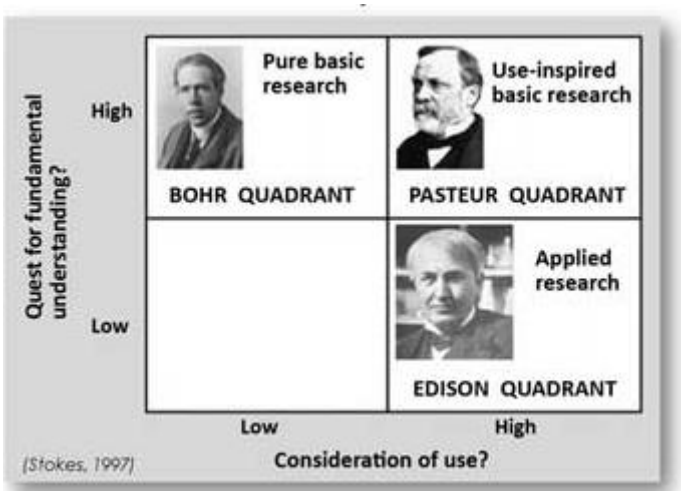

Figure 2-4: Stoke's tripartite division of research. Image Source: Princeton Environment Institute

The JASON project classfies Cyber security in the Pasteur's or the "use inspired basic" research quadrant.

There is also a differing opinion by a growing body of researcher's who propose the Game Theory to address cyber security. The prolific work carried out by the Department of Computer Science in the University of Memphis and the growing band of followers who flock to the GameSec Conference on Decision and Game theory that aims to bring together researchers who aim to establish a theoretical foundation for making resource allocation decisions that balance available capabilities and perceived security risks in a principled manner (Alpcan, 2010). Sankardas Roy et al., in their survey of game theory for network security identify a number of approaches that researcher have taken to based static game models or games with perfect information or with complete information (Roy, et al., 2010). Sajjan Shiva et al., also use Game theory inspired Defence Architecture or GIDA model to build a holistic defence in depth approach to cyber security (Shiva, Roy, & Dasgupta, 2010).

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), who have looked at various components of network security.

The biggest criticism of the Game theory centric apporach is that do not consider a realistic attack scenarios and the complex computational models that serve as a detterent (Roy, et al., 2010).

Laudon and Traver in their book on E-Commerce (Laudon & Trevor, 2015) that has become the default text for any student of E-commerce at a graduate or undergraduate level, propose a very simple 4 layer model for addressing security in the ecommerce world. The security model, elegant in its simplicity is shown in Figure 2-5 below. The data is at the heart of the business in any e-commerce enterprise and forms the core of the assets to be protected. Around this asset are concentric layers of Technology, Organization Policies and Procedures and Laws and Industry standards all of which have a bearing on security in the e-commerce world.

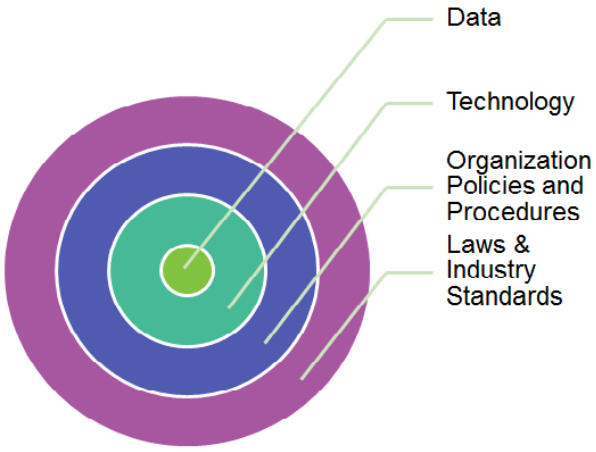

Figure 2-5: Laudon and Traver 4 layer model for Cyber Security Source: (Laudon & Trevor, 2015)

2.9 SUMMARY LITERATURE REVIEW BY THEMES

The reviewed literature can be grouped / summarized into subset of 6 themes

- To establish cyber security vulnerabilities threaten the National Critical Infrastructure (NCI) globally
- India too faces the threat of cyber-attacks on the National Critical Infrastructure
- Amongst all the Critical Infrastructure domains, the Energy sector faces the maximum threats
- Government Mandates and Regulations helps improve security posture
- Advanced / First world countries like the US, EU and UK have an existing or proposed domain specific regulations for the power sector
- Cyber security is nascent domain with little theoretical underpinning and is categorized as Use Inspired Basic Research.

The summary of the Literature Review is depicted in the Table 2-2 below:

Themes / Inference	**Select Authors/Papers**
Cyber security vulnerabilities threaten the National Critical Infrastructure NCI globally	Goodman (2015); Kroger (2008); Hellstorm (2007); Knapp & Langill (2015); Nicholson, Webber, Dyer, Patel, & Janicke (2012)
India too faces the threat of cyber-attacks on the National Critical Infrastructure	Indian Computer Emergency Response Team CERT-In (2007); Indian Computer Emergency Response Team Cert-In (2015); Press Trust of India (2015); Institute for Defense Studies and Analysis (2012);

Themes / Inference	**Select Authors/Papers**
	Information Warfare Monitor and Shadowserver Foundation (2010); Patil (2014); Press Trust of India (2014); Government of India Central Electricity Authority CEA (2013); Government of India Ministry of Communications and IT Department of Electronics and Information Technology (2013)
Amongst all the Critical Infrastructure domains the Energy sector faces the maximum threats	Lee R. M. (2011); Barnes (2010); Langer (2011); Lee R. M. (2011); Hale G. (2011); Zetter, (2012); Ryu Kim & Um, (2009); Falk & Fries (2011); Paul Das Gupta Islam Saha & Majumder, (2012); Wang & Lu (2013); Pearson, (2011); Zhaoyang (2014); Gross (2011); Clemente (2009); Deng & Shukla (2012); Anderson & Fuloria, (2011); Brown A. (2002); Watts. (2003); Byres, (2013)
Government Mandates and Regulations helps improve security posture	Rosenzweig (2011); Hansel (2013); Kobayashi (2011); Nye (2010); Lewis J. A. (2010); Lewis J. A. (2013); Moore (2010) ; Anderson Moore Nagaraja & Ozment (2007)
Advanced / First world countries like the US, EU and UK have an existing or proposed domain specific regulations for the power sector	The White House (2013); North Amercian Electricity Reliabiity Corporation (n.d).; North America Electric Reliability Corporation (n.d).; Malashenko Villarreal & Erickson (2012); Pennyslavania Public Utility Commission (2013); McCabe (2014); Smart grid Interoperability Panel (2014); Smart Grid Interoperability Panel 2010; Euractiv (2013);

Themes / Inference	Select Authors/Papers
	Europeon Commission (2009); European Commission (2013); ENISA (n.d).; ENISA (2011); ENISA (2012); Office of Cyber Security and Information Assurance in the Cabinet Office (2011); Tritschler & Mackay (2011); Tritschler & Mackay (2011)
Cyber security is nascent domain with little theoretical underpinning and is categorized as Use Inspired Basic Research	Brown, Klopp, Palmer & Wolf (2014); JASON, The Mitre Corporation (2010); Stokes 1997; Alpcan (2010); Shiva Roy & Dasgupta (2010); Liang & Xiao (2013); Hespanha (2002); Yi Luo (2010); Laudon & Trevor (2015)

Table 2-2: Summary of Literature Review

2.10 RESEARCH GAP

India, like other countries has brought out its National Cyber Security Policy (Government of India, Ministry of Communications and IT, 2013) and Guidelines for Protection of National Critical Information Infrastructure, (National Critical Information Infrastructure Protection Centre, NTRO, 2013) in 2013 as the apex policy response. The survey of the literature established the lack of domain specific regulations for the power sector in India. A big challenge in the cyber security domain is the surfeit of guidelines, standards and frameworks on security. The UK government research report on cyber security standards points out that there are over a 1000 publications globally that relate to cyber security in one form or other (Department of Business Innovation & Skills, 2013). A focused domain specific regulation for the power sector would help the organizations navigate this maze and improve their security posture.

2.10.1 THEORETICAL GAP

Cyber security is a nascent domain and the theoretical frameworks are yet to be established. The complex and diverse nature of the cyber security world has meant that there is no easy theoretical fit from either the mathamatical, science or other areas. The existing attempts to provide a theoretical model are largely complex and involve significant computational work. There is no equivalent of the Laudon and Traver 4 layer E-commerce security model in the cyber security domain.

2.11 CONCLUDING REMARKS

The survey of literature helped establish that cyber security vulnerabilities threaten the National Critical Infrastructure (NCI) globally and in India. The energy sector has borne the brunt of cyber-attacks and nearly half the attacks on critical infrastructure was directed at the energy sector. The survey of literature brought out the need for government Mandates and regulatory interventions to improve the security posture. Advanced / First world countries like the US, EU and UK have an existing or proposed domain specific regulations for the power sector which is lacking in India.

The review of the literature further brought out that the Cyber security is still a nascent domain with little theoretical underpinning and is categorized as “Use Inspired Basic Research” or Pasteur’s quadrant. Researchers have used game theory to establish the theoretical framework for sections of the cyber security domain like network security. There is no theoretical model for cyber security for critical infrastructure on the lines of the 4 layer Laudon and Traver’s model for e-commerce security.

3 CYBER SECURITY THREATS IN THE POWER SECTOR: NEED FOR A DOMAIN SPECIFIC REGULATION IN INDIA

3.1 OVERVIEW

The R-APDRP (Restructured Accelerated Power Development and Reforms Program) is the national flagship program aimed at building the ICT capability in the Indian utility sector with the objective of alleviating the Aggregate Technical and Commercial (AT&C) losses and improved customer service. While there has been an improvement on both these aspects with the reduction in AT&C and in building an IT enabled infrastructure for customer service, this automation and IT enablement also increases the threat landscape. The chapter highlights key cyber security threats across the entire power sector value chain – from generation, to transmission and distribution – and is aimed at building the case for power sector specific cyber security regulation in India, drawing upon the experience of regulators in other critical infrastructure sectors like Banking and Telecom in India and Power sector regulations internationally.

3.2 INTRODUCTION

The Indian power sector has grown significantly since a small beginning with a miniscule capacity of 1362 MW (Indian Power Sector) at the time of Independence to 210951 MW as on Dec 2012 (Central Electric Authority, 2012). The industry is however plagued with shortage in capacity and high

Transmission and Distribution (T&D) losses. The T&D losses on an all India basis were at 23.97 % and the Aggregate Technical & Commercial losses (AT&C) were at 26.15% for the year 2010 - 11. The peak power shortage is as high as 17.5% in the power starved Southern region and varies from 5 % to 8 % across the other parts of the country (Central Electric Authority, 2012).

The Indian Central Government has initiated a number of structural and regulatory reforms to address the issues in the power sector, including the unbundling of the sector, promoting private sector participation and reduction of the huge AT & C losses. The Electricity (Amendment) Act 1998 and 2003, the setting up of Independent Regulatory authority both at the Federal (Central Electric Regulatory Commission – CERC) and the state (State Electricity Regulatory Commissions - SERC) levels and financial restructuring of the State Electricity Board (SEB) form part of the legal and enabling framework to address the shortcomings in the Indian Power Sector.

The Smart Grid roll out in India is one other step aimed at addressing the problems in the Power Sector. Quality Power on Demand for all and Transform the Indian power sector into a secure, adaptive, sustainable and digitally enabled ecosystem by 2027 that provides reliable and quality energy for all with active participation of stakeholders is the lofty mission and vision that the National Smart Grid Mission (NSGM) has set out to achieve for itself (India Smart Grid Forum, 2012).

With a planned outlay of INR 31,500 Crores (approximately USD 5.8 Billion) in the National 12th Five Year Plan Period between the FY 2012 – 17 the Smart Grid Mission and success of smart grid roll outs is critical to the well-being of the Power Sector in India

The R-APDRP or the Restructured Accelerated Power Development Program was launched in 2008 in the XI Five year plan period. The flagship program launched by the central government to aid the utilities to baseline customer data, adoption of IT, reduce AT&C losses and to upgrade the Distribution and Sub-

Transmission network. R-APDRP with a budget outlay of INR 3114 Crores (Ministry of Finance, Government of India, 2013) (approximately USD 576 Mill) for the fiscal year 2012-13 would also lead to significant investment and upgrade of IT Infrastructure in the Indian Power Sector.

While the technology behind the smart grids is expected to usher in a new era and revolutionize the industry and impacts every point of the value chain from metering, to distribution and transmission, it (Technology) however can also be the Achilles heel, as the cyber world is as susceptible to threats like in the physical world.

Cyber threats / attacks have evolved over a period of time. If the popular early image of the hacker was of a "geek" or a precocious kid popularized by various Hollywood movies, this has since evolved. The motivation of attackers moved on with time driven by financial gain and then organized well established market place for trading in malware and stolen credit card data to now where attacks that are aimed at crippling the National Critical infrastructure (NCI) and creating mayhem. While most of the early Cyber-attacks and breaches have been motivated by financial gain, targeting banks and credit cards for example, in the recent past however there has been increase in instances where the nations electric grid (Date, 2010), power and utilities (Brown G. D., 2011) have been the target of cyber-attacks. There have been a number of international cyber security incidents like in Baltic (Tikk, Kaska, & Vihul, 2010) across Estonia in 2007, Lithuania and Georgia in 2008 where the country's infrastructure has been target of concerted attacks crippling the infrastructure. This evolution has also meant that the cyber threats have become more sophisticated and the impact caused by these cyber-attacks has become more and more damaging. Refer Figure 3-1 below.

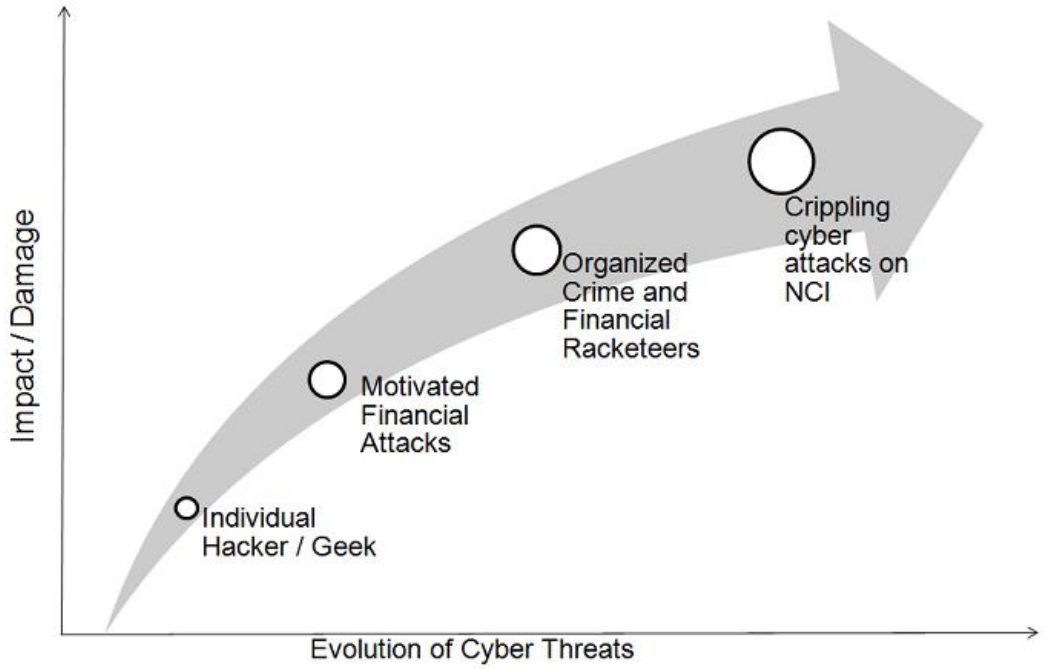

Figure 3-1: Evolution of Cyber Threat and Impact

In the case of national critical infrastructure, threats can also be from nation states which are inimical and who have significant resources at their disposal. India has been no exception to this and has faced a barrage of cyber-attacks (Cert-In, 2011). With widespread introduction of information systems in the power sector, this sector might increasingly become an easy target for cyber attackers. The emergence of smart grids and vulnerabilities to SCADA systems, which were all along seen as immune to cyber threats, would only increase the threat exposure in the power sector.

Given the unique nature of Power sector and the threats targeting this domain and the fact that a successful attack on the key organizations / installations in this domain can bring the nation down to its knees, there is need to evolve a comprehensive Cyber security policy and regulatory response to address the specific cyber security needs of Power Sector in India.

A safe and secure Cyberspace is the substratum that provides the foundation for the well-being of the power sector. However protecting the cyber space poses a number of challenges.

3.3 CYBER SECURITY - KEY CHALLENGES

As a chieftain, responsible for the security of the fort in 18th century, who has built high walls, lined with cannons, dug the deepest of moats infested with frightening beasts and soldiers armed to drive away the enemy attacking from the ground, is helpless when the enemy glides in over the air – so too is the impact that cyber-attacks bring to bear on the traditional critical infrastructure protection strategies and plans.

Cyber-attacks provide potential aggressors, whether nation states, non-state actors or terrorists yet another option to perpetrate their evil designs, and many a times cyberspace could potential prove to be an easier target. Terrorists and unfriendly nation states have long realized that it is far easier to get away with the attacks on the nation's cyber infrastructure than an attack in the physical world (Clemente, 2009). This could be no different in the Indian context.

This is because, Cyber Security and response to Cyber threats poses more than one challenge. Highlighted below are the select few:

1. Appreciation of the threat itself

   It is easy to under estimate the exposure or damage that can be brought about by the cyber threat. When building applications, devices or systems the developers are focused on addressing functional requirements and non-functional requirements like security can take a back shift. A SCADA system that controls the gas pipeline which has been compromised can be rigged to increase the pressure to dangerously high levels leading to explosions. Similarly the smart grid network that has been taken over by a BOT can disrupt the entire grid.

2. Challenges in the discovery of the exposure / threat

   There have been a number of cases where the breach or exposure was not discovered for months together or well after the incident. In the TJX breach, where the company lost credit card data of 45+ million customers and faced a loss running into millions of dollars, it is estimated that the breach was running from July 2005 to Jan 2007, before it was detected in Jan 2007 (TJX Securities Exchange Commission Filing).

3. Attribution or Identifying the perpetrator or the source of the threat
   Many a times, even subsequent to the discovery of the incident, it is exceedingly difficult to point the source of the attack as it can be masked to come from different countries or even from within the country. The spread of botnets and command and control infrastructure with sleeper cells spread globally and that can be remotely activated, adds to the complexity.
4. Determining the appropriate response
   Incident management and threat response is key and organizations are seldom as well prepared to cyber incident as they are to a physical incident. Whether it is responding to a credit card loss or targeted D-DOS attack – there is need to have well-structured incident response to ensure that there is Business continuity and the confidentiality and integrity of the critical assets are not compromised.
5. Jurisdiction
   Policy formulation and regulatory response to Cyber Security is often mired in turf and jurisdictional overlap. There would be a need to bring together and deliver a coordinated response to Cyber threat. There are a number of stakeholders who would need to be involved to respond to a cyber-attack targeting the Power Sector – a partial list is below
      i. Ministry of Power – the nodal ministry for the E&U sector

ii. Ministry of Home Affairs as it involves internal security
iii. CERT IN
iv. Ministry of communication and Information Technology and Department of Telecom (DOT)
v. National Disaster Management Committee
vi. Ministry of Defence – if it involves external aggressors
vii. Industry players

6. Lack of International Legal Framework

   Given that there is today even a disagreement on how ICANN (Internet Corporation for Assigned Names and Numbers) needs to be governed – under the UN if we go with the argument extended by Indian and other BRIC countries or to retain status quo as argued by US and the developed world who have a vested interest in ensuring there is no change, the likelihood of a global convention on cyber security indeed seems to be a far cry. The lack of a global agreement, and plausible deniability and inability to pin point the perpetrator, makes cyber warfare an attractive option to the aggressor.

In India, the primary legal framework to address the cyber security concerns is the IT Act of 2008 and relevant sections of the Indian Penal code.

In the power sector, these challenges are further compounded by sector specific nuances. Cyber security needs to be ensured both across the corporate IT systems and the Control Systems. Both these domains are unique and differ in their issues and in its solutions. The security gaps and threats in the corporate IT world of the power sector would be similar to that across other sectors and generic security solutions that work in other verticals would be well suited to address the security concerns here. The control system security however would need an appreciation of the both the domain and security. The power sector can be broadly classified into three sub segments – Generation, Transmission and Distribution. Security vulnerabilities exist across all the three segments. The subsequent section discusses the threats specific to these segments.

3.4 SECURITY VULNERABILITIES IN POWER INDUSTRY VALUE CHAIN

Conventional wisdom even till a few years ago focused on cyber threat vulnerabilities on the transmission system alone. The rationale being that Generation Systems are usually remote and not open and largely not connected to the Internet and this isolation itself would provide the Gen Cos the security from cyber threats. On the other hand, at the distribution level, the argument went that even if there was a compromise and breach, the ability to create damage would be localized and impact minimal. Thus there being no incentive for the potential attacker if his goal was to create large scale damage. However, the entire value chain in the Power Sector has been proven to be susceptible and a number of incidents in the recent past have exposed the vulnerabilities in each of the sub-sectors in the power industry.

3.4.1 THREAT EXPOSURES IN GENERATION SYSTEMS

A number of research studies have documented the vulnerabilities found in SCADA systems and these include hardcoded passwords, backdoors, and passwords in clear text, lack of strong authentication solutions, firmware vulnerabilities and Ladder Logic amongst others. Dale Peterson and his team of researchers announced list of vulnerabilities in almost all leading and widely used PLC (Programmable Logic Controllers (PLC) in Jan 2012 (Zetter, Scada Exploits, 2012).

The list of vulnerable products with one or more security vulnerabilities identified in the study includes

1. General Electric D20ME
2. Koyo/Direct LOGIC H4-ES
3. Rockwell Automation / Allen Bradley ControlLogix
4. Rockwell Automation / Allen Bradley MicroLogix

5. Schneider Electric Modicon Quantum
6. Schweitzer SEL-2032 (communication module for relays)

Just six months prior to this, an individual security researcher Luigi Auriemma, a self-confessed novice in the SCADA domain, published 34 exploits that target seven vulnerabilities in SCADA systems made by Siemens, Iconics, 7-Technologies and DATAC (Hale, 2011). While the level or impact of these vulnerabilities is debatable, the point remains that an individual researcher, with minimal prior experience on SCADA was within a short period of time, able to identify and exploit vulnerabilities in the control systems.

By far the most well-known cyber-attack and variously called the "Hack of the Century" or the "First Deployed Cyber Weapon in History" is Stuxnet. Stuxnet is clearly one of the most sophisticated and most expensive malware produced and much like a modern missile that can navigate through the air and strike at a specified target (Gross, 2011), Stuxnet in the wild seeks out specific target systems and triggers the payload only on specific conditions. Its sophistication stems from the fact that it covers not only its tracks and hides its presence, but also the effect of the payload until well after the damage is done. Ralph Langner, Control systems Security Expert was the first to arrive at the conclusion that that the Stuxnet virus, was targeted at the PLC running the centrifuges in Iran's Nuclear Plants, in Bushehr and Nantaz. Based on his research on Stuxnet, he also goes on to speculate that the malware was funded and built by US and Israel (Langer, 2011).

3.4.2 THREAT EXPOSURES IN TRANSMISSION SYSTEMS

Historically Transmission systems have been by far the most targeted subsystem in the Power System Value chain. Over a 10 year period 1994 – 2004 for, transmission systems accounted for over 60 % of the target for attacks on the Electric Grid (Clemente, 2009). Details in Figure 2 below.

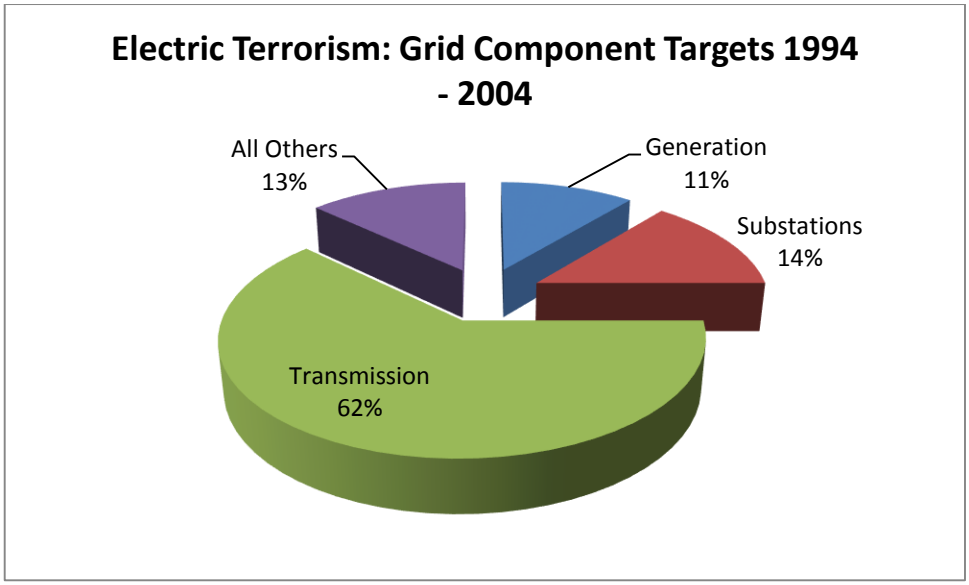

Figure 3-2: Electric Terrorism: Grid component Targets 1994 -2004

Others include distribution, electric relays, human resources, and junction boxes.

One of the most prominent attacks on the transmission network is linked with the Trans-Siberian Gas Pipeline. This gas pipeline was (and continues to be) the lifeline of the then Soviet (now Russian and Ukrainian) economy and a key source of hard currency earnings. The Trans-Siberian gas line network is 4500 kilometres long and with a capacity of over a trillion cubic feet of gas supply in a year (Urengoy Pomary Uzhgorod Pipeline, n.d.). In 1982, a huge explosion rocked the pipeline. It was the largest non-nuclear explosion in the history and apparently even visible from space (Hoffman, 2004). Writing in his memoir, At the Abyss: An Insider's History of the Cold War, Thomas C. Reed, a former secretary of the Air Force and special assistant to President Reagan, provides a detailed account of how, an American Intelligence operation was responsible for slipping in a Trojan into the control system software of the pipeline that lead to malfunctioning of the equipment's and causing the explosion. While this theory has its detractors and like most intelligence activities can never be confirmed, the cyber-attack theory is definitely a plausible explanation of the explosion.

While many of the vulnerable PLUs identified in the previous section will also directly impact on the SCADA systems used in the transmission subsystem, there are a number of other cyber vulnerability exploits that can impact the transmission subsystem. The relays on the Transmission subsystem are time sensitive and delays of even few milliseconds can have an impact on the performance and change the desired outcome. The common D-DOS or Distributed Denial of Service attack can flood the network and communication channel increasing the response time delays and cause the malfunction of the smart grids.

Deng Yi and Sandeep Shukla in their research note have identified a number of different channels that is available to the perpetrator, including Malicious Data Injection by compromising the Meters and introducing state estimation errors arbitrarily which escape detection by the of the current bad data detectors (Deng & Shukla, 2012).

3.4.3 THREAT EXPOSURES IN DISTRIBUTION SYSTEMS

Smart meters or Advanced metering Infrastructure is expected to revolutionize the way we consume and pay for electricity. With the ability to track and report on consumption by the minute and is key to introducing Time of the Day billing, reduce the meter reading effort and improve efficiency.

Smart Meters are IP devices connected to the network via one or more type of communication links. Smart meters apart from meeting functional and non-functional requirements like performance would need to incorporate basic security features like authentication and encryption. Smart meters connect to the central control or Network Operating Centre (NOC) room of the utility to transmit data and receive "instructions" – poor security implementations in the smart meters could make it possible for an unauthorized third party to "impersonate" the NOC. The consequence can be disastrous if the meter has the "switch off" capability. Given the sheer volume involved and number of units involved which for large utilities could run into millions of smart meters,

security vulnerabilities post roll out would result in issues of magnitude never before managed by the utilities.

Patching or fixing security vulnerability once the meters have been deployed, can run into millions of dollars. It is estimated that replacing 100 Million meters, would cost up to USD 20 billion and 5 years of time (Anderson & Fuloria, Smart meter security: a surver, 2011). At the basic minimum, smart meter vulnerabilities can help the consumer get away without paying for electricity they consume and at the other end of the spectrum, if a state actor or aggressor gets access to control millions of electricity meters with the ability to plunge the country into darkness at will, could cause significant damage.

There is evidence to show that not all meter manufacturers have factored security into their design, C4 Security, in their white paper, The Dark Side of Smart Grid – Smart Meters (in) Security identify basic security issues in the smart meters that they have studied (c4 Security). In their study of the meters that have been deployed, the team found fundamental issues that feature in the OWASP top 10 including

1. Lack of Authentication
2. Authentication Bypass
3. Slave meter data tampering (quite similar to the Man In The Middle or MITM attack in the web world)
4. Insecure Protocol Implementation
5. Input Validation Errors

Security considerations for Smart Meter should factor in Tamper protection and detection, Interface and configuration review to detect default passwords and protocols in clear text, Micro-controller dumping and EPROM (Erasable Programmable Read Only Memory) dumping testing amongst others (Ernst & Young, 2011).

3.5 DATA PRIVACY AND CUSTOMER PROTECTION

While the security exposure in the grid needs attention and the focus to secure the grid against attacks aimed at disabling the critical infrastructure. There is another aspect of security that needs attention and mitigation. Smart grids generate tons of data about consumers, their electricity usage habits, consumption patterns and other PII (Personally Identifiable Information) data. This data in wrong hands can be misused and be the cause of potential mischief. Analysis of usage patterns of the consumer can reveal whether a person is at home or away for example or what kind of devices are being used etc. Unlike in the Telecom industry, where there are strict regulatory controls on consumer data and who has access to customers CDR (Call Data Records) or have access customer sensitive information, there are no such regulations in the utility industry.

3.6 ZERO DAYS AND ADVANCED PERSISTENT THREATS

While Zero days and APTs (Advanced Persistent threats) get the maximum coverage in the press and management attention, from the experience of the authors, there are more basic issues that most security managers in utilities need to address first before they splurge on the latest tool to track down and prevent Advanced Persistent Threats or focus on fixing the newest Zero Day Patch.

The security threat assessments that the authors have been involved with a number of global utilities have shown startling gaps - starting with lack of basic network zoning, access control deficiencies, privilege escalation vulnerabilities, default passwords, and patch updates that are not current. This is corroborated by the findings of Jonathan Pollet, who reports that in his study and assessments of over 100 SCADA environments, it was quite common to find systems that were anywhere between one to three years behind in their patching schedules (Pollet, 2010). The Aug 2012, Saudi Aramco breach on the corporate

IT systems showed that many of the security devices were on default passwords (Zorz, 2012).

Thus while it is tempting and it is probably easier to get the organization to write a cheque when there is a breach or when the newest zero day receives attention, money is better spent elsewhere.

While a significant sum of money is to be spent on upgrading the ICT infrastructure in the power grids in India, a systematic and risk based approach to cyber security would help mitigate the cyber security risks. From National Critical Infrastructure (NCI) perspective, it is important to ensure that various players in the Industry have at least a minimum baseline of security. A standard or compliance mandate would be one step to help attain that state.

3.7 REGULATORY FRAMEWORKS AND STANDARDS FOR CYBER SECURITY

The authors' empirical experience over the many years has shown that security spend has been closely tied to either a regulatory requirement or a compliance mandate. This is probably because Return on Security Investments is often difficult to establish or there is a lack of clarity of the security issues at the board level. From implementing the IT controls as part of SOX (Sarbanes–Oxley Act of 2002) compliance requirements, Industry compliance requirements like PCI-DSS (Payment card Industry Data Security Standards) for credit card protection, or regulations in financial services Industry, mandated by various central banks including the likes of Reserve Bank of India (RBI), Monetary Authority of Singapore (MAS) that have driven various security implementations including Multi Factor Authentication, Application Security Testing and security guidelines for banking. Bruce Scheiner, author and security guru, reflecting on a decade of security trends, reminiscences that it is the Regulatory mandates

including the likes of SOX, HIPAA, GLBA, PCI and the various data protection acts and breach laws are what forces companies to take security more seriously (Mimoso, 2008). This section looks at the regulatory framework in other sectors of NCI in India and power sector internationally.

3.8 CYBER SECURITY REGULATIONS IN OTHER (NON POWER) NCI SECTORS IN INDIA

While the cyber security regulation in India in Power Sector is still nascent, there is a history of cyber security regulations in other areas of National Critical Infrastructure in India.

The RBI has been the most proactive amongst the regulators in India when it comes to driving IT Security amongst its regulatees, natural probably, given the sensitivity of security in the Industry which they operate in. RBI guidelines and polices on Information Security in Banking has been setting the standards for the banking industry in India and has been instrumental in enforcing better security standards in India. Starting as early as 2001, with the Internet Banking in India Guidelines (Reserve Bank of India, 2001) mandating Technology and Security Standards and continuing to keep pace with evolving technology and risk with security being the focus in the recommendation of the Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds in 2011 (Reserve Bank Of India, 2011) – Implementation of Recommendation, April 2011. Similarly information security is key component of the RBI Mobile Payment in India - Operative Guidelines for Banks. The Survey on Banking, Financial Services & Insurance Industry, in 2011 points out that RBI Guidelines and other compliance requirements like Basel 3 drives 50% the investments in IT Security (Symantec Corporation, 2011) in banking domain in India.

The telecom sector in India has similarly seen security mandates and guidelines incorporated as part of its licensing terms for operations and policy mandates.

The May 2011 (Government of India, Ministry of Communications & IT, Department of Telecommunications (Access Services Wing), 2011), amendment to the license terms for operation under the UASL (Unified Access Service License) mandates numerous security controls and compliance requirements on the licensee to address security needs across networks, devices, access and applications. The NTP-2012 (National Telecom Policy 2012) provides for localization and indigenous manufacture with complying with specific security standards, security certifications labs and security standards across all the building blocks in the Telecom networks (Government of India, Ministry of Telecommunications & IT, Department of Telecommunications, 2012).

There is therefore a precedence and significant learning that the Power sector can gain from the other sectors and focus their energy on areas that are peculiar to the sector like control systems and distribution networks.

3.9 CYBER SECURITY REGULATIONS AND MANDATES IN POWER SECTOR IN SELECT COUNTRIES ACROSS THE WORLD

There are largely two different approaches to regulations in the Power Sector – the U.S. approach which is largely focused on voluntary reporting mechanisms and on the other hand, E. U. that is taking a more compulsory compliance approach with the European commission measures to ensure harmonized network and information security across the EU (Euractiv, 2013).

The U.S. regulations on power sector is primarily governed by the NERC – CIP (North America Electric Reliability Corporation - Critical Infrastructure Protection) mandates and the standards evolved from the NIST (National

Institute of Standards and Technology) and more specifically from the NIST Interagency Report (NISTIR) 7628, Guidelines for Smart Grid Cyber Security.

NERC-CIP however has its limitations; the Federal government mandated NERC CIP guidelines only cover the bulk electricity system which is regulated by the Federal government. The states are expected to fill the vacuum from the gaps in the federal regulation. The state regulators including the likes of California Public Utilities Commission, Colorado Public Utility Commission and the Texas Public Utility Commission have promulgated rules to protect customer privacy and data generated by Smart meters (Malashenko, Villarreal, & Erickson, 2012).

The E. U. Directive concerning measures to ensure a high common level of network and information security across the Union (European Commission , 2013) aims to provide for a high common level of network and information security. The objective is to ensure that there is a structure for cooperation between nation states and also framework and guidelines for the operators of critical infrastructure, including Energy companies to manage security risks and reporting of critical incidents within the state.

Apart from the E. U directives the member states have their own internal regulatory requirement or policy guidelines or standards. A snap shot is provided in the Table 1 below (ENISA - European Network and Information Security Agency, 2012).

In the Indian power sector however, cyber security regulations or mandates are conspicuous by its absence with both the National Electricity Policy (NEP) and Electricity Act 2003 and its amendment in 2007, not even making a fleeting reference to cyber security.

Given the potential damage that can be caused by a cyber-attack on the power grid can cause to the India, this needs to be remediated.

Country	Name	Type
The Netherlands	Privacy and Security of Advanced Metering Infrastructure	Guidelines
France	Managing Information Security in an Electric Utility	Guidelines
Germany	VIBE R175. IT security for generating plants	Guidelines

Table 3-1: Country specific Information Security Guidelines for Power Sector in E.U

3.10 OTHER RELEVANT IT SECURITY REGULATIONS AND STANDARDS

Apart from the sector specific regulations and standards, the corporate IT arms of the global Utilities have invested significantly on shoring up their cyber security as they need to comply with other regulations. Large utilities listed in the USA face compliance mandates like SOX (Sarbanes-Oxley Act, 2002) and PCI-DSS. IT security and control implementations that have been made to meet these compliance norms over the years have helped these organizations address a number of their security lacunae in their corporate IT systems. Players in the Indian power sector do not start with this advantage either with none of the SEBs listed and with generation companies and grid companies also not having to comply with these norms either.

3.11 CONCLUDING REMARKS

The smart grid is seen as a panacea to rid the Indian Power sector of its ills, and thousands of crores (1 Crore = 10 Million) have been earmarked to achieve this

goal. Upgrading the ICT infrastructure in the power grids without proper security planning and addressing key risks, are likely adding to the misery that the industry is facing, apart from increasing the risk exposure to the national critical infrastructure. This is definitely not an attempt to debunk the benefits of the Smart Grid or even an opposition to the smart grids, this is more a call to appreciate the security risks that the smart grid poses to the national critical Infrastructure and the need to carefully assess the security risks, and evolve a national policy or regulatory framework to address these issues.

While there is certainly no lack of relevant standards to address cyber security vulnerabilities in general, and there are sufficient technology controls to address cyber risks, there is always a cost vs. risk acceptance trade off. From a risk management perspective, cyber incidents in the power grid pose a number of challenges. There are some areas like customer data breach or the lack of availability of critical IT system where the Annualized Loss Expectancy (ALE) could be readily calculated, whereas in other areas, for example a breach of control systems like in the case of Stuxnet incident would pose challenges. Security investment decisions based on ALE, would typically not address high impact but very low probability incidents. It would be very difficult of the CISO (Chief Information Security Officer) to build a business case for such investment decisions. This is aggravated further in the Indian context with the SEBs already in dire financial state.

The same view is echoed by James Lewis, director of the Technology and Public Policy Program at Centre for Strategic and International Studies (CSIS), in relation to the AGA – 12, data communication encryption standards which was not adopted by the utilities because of cost. He points out that while the players know what is required to address or enhance security, they do not implement it because it does not make business sense or provide commercial gains, thus rendering the voluntary approach impractical (Malashenko, Villarreal, & Erickson, 2012).

The security policy / standard for the Power Sector should address the entire spectrum of cyber security including

1. Security Policy and Management
2. Security Organization
3. Security Mandates for the Corporate IT Systems
4. Domain Specific security standards for Control Systems
5. Business Continuity Planning and Disaster Recovery
6. Customer Data Protection
7. Physical Security Requirements
8. Periodic Assessments and Reporting
9. Data Sharing and Collaboration

While there is a wealth of knowledge and learning that we can leverage, both from the experience of other domains in India and the power sector globally, the nuances around Control System security, Data Sharing and Collaboration that would have to be specific to the nation's power sector.

Figure 3-3: Key Components: Cyber Security Power Sector

The cyber threat and issues are too serious to be left laissez-faire to the industry players alone and yet the government alone too cannot solve all the problems. Cyber security would need to be treated at par with other resiliency requirements of any grid planning exercise.

While there is no guarantee of a 100% security, mandatory regulatory compliance requirements would establish a basic level of security standards across the entire industry value chain. This combined with continuous internal monitoring and a clearly defined incident response approach, collaborative information sharing within the Industry and government agencies like CERT-In can go a long way in reducing the risk exposure

A national policy doctrine to address cyber security for national critical infrastructure and a regulatory framework that provides guidance to the industry players across generation, transmission and distribution would be a first step to address the cyber security issues that the Indian Power Sector faces.

4 RESEARCH DESIGN

4.1 OVERVIEW

Research design is the blueprint that details out how the researcher intends to achieve his end objective. It includes the research methodology, the approach to collection, measurement and interpretation of data. The research design needs 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 identifies 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 also delves into the rationale and 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 and validity of the research design.

4.2 INTRODUCTION

The research design provides a framework for the collection and analysis of data (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 part of the investigation
- Understanding behaviour and its meaning in a specific context
- Having a temporal appreciation of a social phenomena

Claire Sellitz et al., add another dimension to research design – economy in procedure { (Sellitz, 1962) as cited in (Kothari C. , 2013)}. Research design is essentially a blueprint for the collection, measurement and analysis of data.

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 decision or conducting 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 carry out the research.

Kothari suggests that Research design can be categorized as

1. **Exploratory research:**
   Is aimed at formulating the problem for more precise 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 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 during the course of the research. Exploratory research design

typically involves one of the three approaches that is depicted in the Figure 4-1 below

i) **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 would help and help formulate the hypothesis for the proposed research.

ii) **Experience Survey** – that involves the survey of people who have a practical experience on the subject

iii) **Analysis of "insight-stimulating"** example – that involves intensive study of the phenomenon of interest.

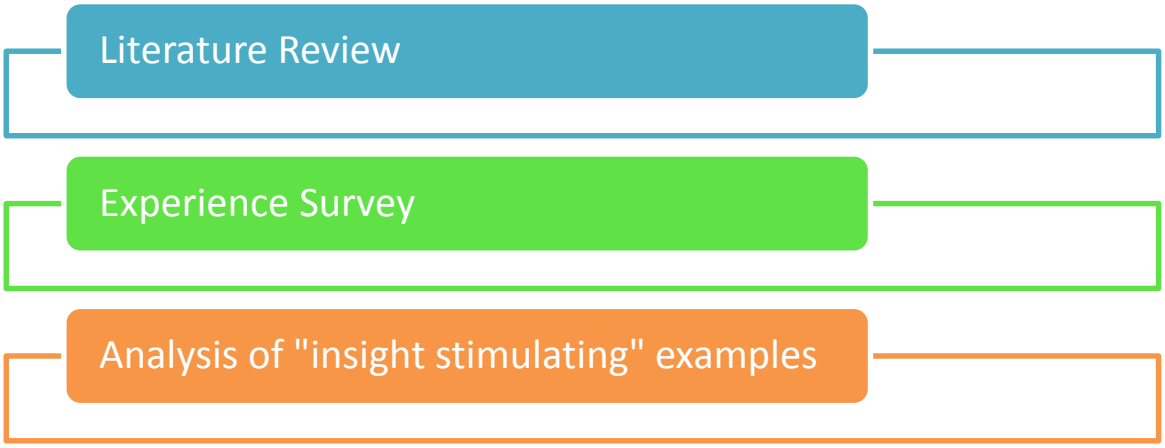

Figure 4-1: Research Design for Exploratory research. Source (Kothari C. , 2013)

Descriptive and Diagnostic Research are more rigid, prevent bias and ensure reliability. The design, as shown in Figure 4-2 below, must focus on

i. Formulating the objective
ii. Defining the methods to collect the data
iii. Defining the sample
iv. Collecting the data

v. Data Analysis

vi. Conclusion

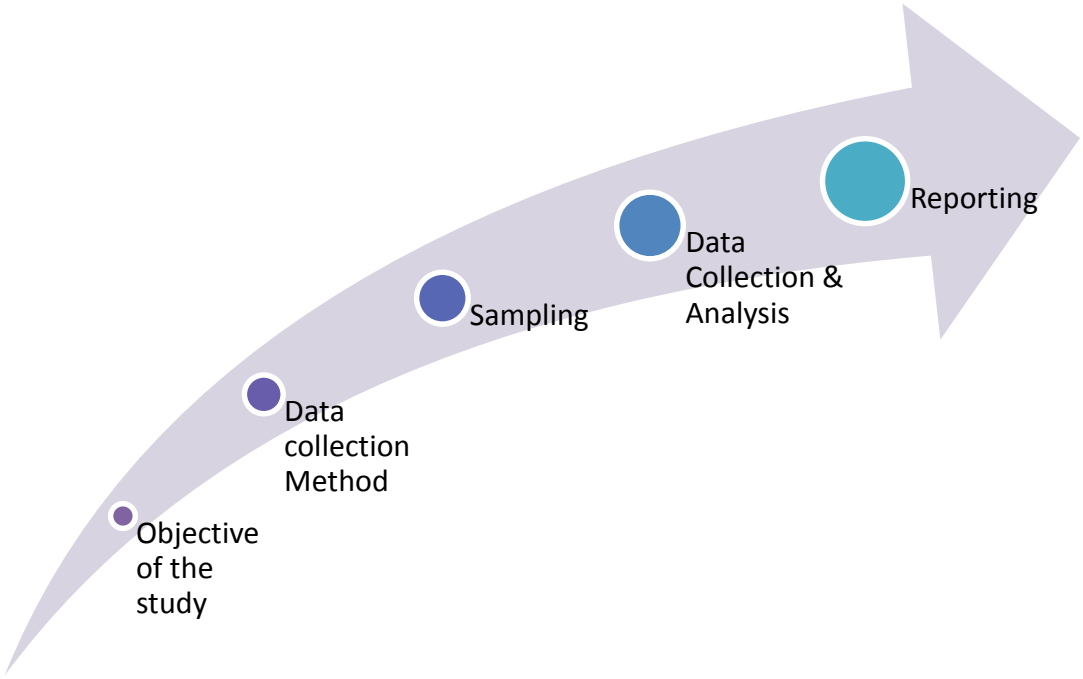

Figure 4-2: Research Design for Descriptive & Diagnostic studies. Source: (Kothari C. , 2013)

4.3 RESEARCH STRATEGY

Research Strategy can be classified as **Quantitative** and **Qualitative**. At a superficial level the difference between the two strategies is often construed as quantitative research as those that involve measurement and qualitative research as those that do not involve measurement (Bryman & Bell, Business Research Methods, 3/e, 2011). There are fundamental differences with different epistemological and ontological considerations.

Quantitative Research Strategy emphasizes quantification in the collection and analysis of the data and entails a deductive approach with a focus on testing of theories. It embraces positivism and views social reality as an external and objective reality. The principal orientation of quantitative research with respect to the role of theory in relation to research is "**Deductive" or testing of theory.**

Qualitative Research Strategy emphasizes words rather than quantification and is predominantly inductive in approach to relationship between theory and research. Qualitative research rejects positivism and embodies a view of social reality as a constantly shifting emergent property of individuals' creation. The principal orientation of qualitative research with respect to the role of theory in relation to research is "**Inductive" or generation of theory.**

Bryman and Bell go on to point out that while the above characteristics are generally true, there are exceptions with example of qualitative research being used to test theories rather than generate them. Qualitative and Quantitative Research also have different philosophical orientation.

The two research strategies articulated Qualitative and Quantitative co-exist in a **Mixed-Methods Research**. Bryman and Bell point out that while there are a number of nay-sayers who argue against mixed-method or multi-strategy research, this approach to business research has gained popularity and a significant number of research scholars have adopted mixed-method research and has seen a three-fold increase in the number of articles in the period decade ending 2003 and between 10 to 20% of the empirical research leverage mixed method research (Bryman & Bell, Business Research Methods 3/e, 2011).

Mixed method research can be classified based on (i) Priority and (ii) Sequence. Thus there are potentially nine different approaches to mixed methods research. 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 (Bryman & Bell, Business Research Methods 3/e, 2011). All the options are captured in the

Figure 4-3 below 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.

Figure 4-3: Mixed Method Research Classification Source (Bryman & Bell, Business Research Methods 3/e, 2011)

In this research the qualitative analysis is executed first using the Framework Analysis with the objective to understand the cyber security challenges in the power sector to answer the first research question. This is followed by the detailed quantitative analysis using Exploratory and Confirmatory Factor Analysis to answer the central research question.

4.4 RESEARCH PHILOSOPHY – EPISTEMOLOGY AND ONTOLOGY

Epistemology answers the question on what is acceptable knowledge in a discipline. The central issue is whether social sciences can be studied according to the same principles and procedures as employed in natural science. The position that advocates the application 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 behaviour. This is termed as **"Interpretivism"** (Bryman & Bell , Business Research Methods 3/e, 2011)**.**

Ontology deals with the nature of social reality. **Objectivism** is an Ontological position that holds that the social phenomenon and their implications independent of social actors. The alternate view or Ontological position is called as **Constructionism** or **Constructivism** (Bryman & Bell, Business Research Methods, 3/e, 2011). Proponents of constructivism argue that social phenomena and their meanings are continually being accomplished by the social actors. Social phenomena and their categories are produced through social interaction and are in constant change.

In conclusion business research is influenced by a number of factors that is shown in Figure 4-4 including Theory, Epistemology, Ontology, Values, and Practical consideration.

Figure 4-4: Influences on business research. Source (Bryman & Bell, Business Research Methods, 3/e, 2011)

The first step of any business research is to define the research problem.

4.5 RESEARCH PROBLEM

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

- The lack of domain specific regulations for the power sector in India.
- Cyber security is a nascent domain and the theoretical frameworks are yet to be established. Laudon and Traver define a 4 layer model for security in the ecommerce sector. The core of the 4 concentric layers is the "Data" and the other layers are technology, organisational polices and proceedurs and Laws and Industry standards.

The research problem for this study is therefore:

"To adapt the 4 layer Information security framework to identify constituents of the cyber security mandate for the Indian power sector"

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

4.6 RESEARCH QUESTIONS

Research Question (RQ 1)

What are the cyber security challenges in the Indian power sector?

Central Research Question (CRQ)

What are the relevant factors that enhance cyber security and their significance in the Indian power sector?

The primary or central research question is to determine the relevant cyber security factors and establish their significance in the Indian power sector. In terms of the sequencing however, the study first focused on eliciting the cyber security challenges that affects the Indian power sector and subsequently

identifying the factors and their relevance to the sector. The Research Question leads to the Objective(s) of the Research.

4.7 RESEARCH OBJECTIVES

The research objectives are aligned to the two research questions as discussed above. The Objectives of this research are:

Research Objective 1 (RO 1)

To find out the Cyber security challenges in the Indian Power Sector.

Research Objective 2 (RO 2)

To determine the relevant factors those enhance the cyber security and test their significance in the Indian Power Sector.

The Research Design provides a systematic approach to address the Research Objectives.

4.8 RESEARCH DESIGN TO ADDRESS OBJECTIVE 1

As discussed in the previous section, this research study utilises mixed methods research with a priority on quantitative techniques and a sequence of qualitative research followed by quantitative research. The choice of research design to address Objective 1 is articulated in the Table 4-1 below.

The Qualitative Research Strategy as discussed by Bryman and Bell (Bryman & Bell, Business Research Methods 3/e, 2011) propose a sequential approach to undertaking qualitative research as show in Figure 4-5 below.

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

Table 4-1: Objective 1- Choices in this research

The research starts with the general research question which in this research is to find out the cyber security challenges in the Indian power sector and has the following sequential steps:

- Selecting the relevant site(s) and subjects,
- Collection of relevant data
- Interpretation of data
- Conceptual and theoretical work
- Writing up the findings / conclusions

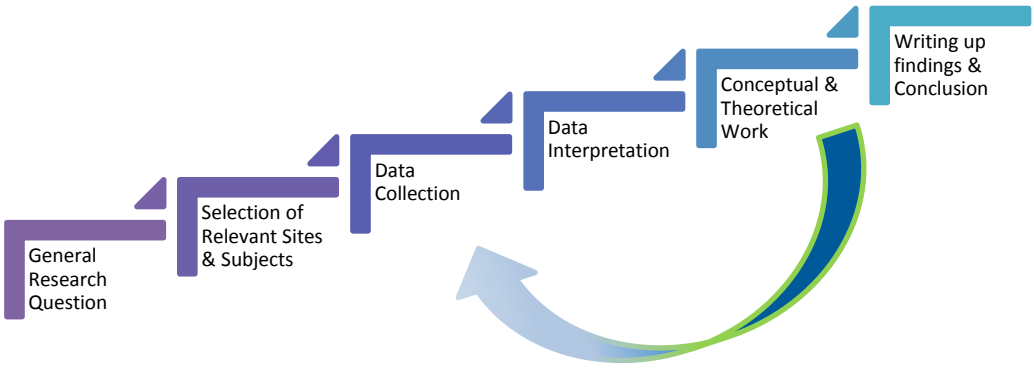

Figure 4-5: Outline of Qualitative Research Steps: Source (Bryman & Bell, Business Research Methods 3/e, 2011)

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

4.8.1 SELECTION OF RELEVANT SITE(S) AND 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 Power Sector and the cyber security domains, members of the office of the National Security Advisor (NSA), service providers and suppliers from both the Power sector and Security industry.

The approach to sampling and Selection of the respondents are discussed in the subsequent sections.

4.8.2 APPROACH TO SAMPLING AND SAMPLE SIZE

Sampling in qualitative research often involves purposive sampling. Bryman and Bell postulate that probabilistic sampling is not appropriate in qualitative analysis (Bryman & Bell, Business Research Methods 3/e, 2011). They recommend that sampling be continued till **Theoretical Saturation** is achieved. Theoretical Saturation implies that successive interviews/observations have formed the basis for the creation of a category and confirmed its importance. Strauss and Corbin suggest that theoretical saturation would mean that no new or relevant data seem to emerge, category is well developed and relationships among the categories are established { (Strauss & Corbin, 1998) as cited in (Bryman & Bell, Business Research Methods, 3/e, 2011)}.

4.8.3 COLLECTION OF RELEVANT DATA

The Interview is the most widely employed method in qualitative research (Bryman & Bell, Business Research Methods 3/e, 2011) for collection of data. Minichiello et al., define **In-depth Interviews** as "repeated face-to-face encounters between researcher and informants directed toward understanding informant's perspectives on their lives, experience or situations as expressed in their own words" { (Minichiello, Aroni, Timewell, & Alexander, 1990) as cited in (MacDougall & Fudge, 2001)}.

Bryman and Bell (Bryman & Bell, Business Research Methods 3/e, 2011) call out the various characteristics of qualitative interview as:

- Qualitative interview tends to be much less structured and the focus is on greater generality in the formulation of the interviewees' perspectives.
- 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

Bryman and Bell identify two major types of interview - **Unstructured and Semi-structured interview**. In the latter the researcher has a list of questions on specific topic 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 flexibility to adapt the respondent's answer. The Interview Protocol is series of memory prompts, questions or visual cues that allow 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 cyber security regulations / standards in the power sector and the initial short list of variables that emerged from the literature review. This is depicted in the figure 4-6 below.

Figure 4-6: Building the Interview Protocol

4.8.4 INTERPRETATION OF DATA

Coding is the first step in analysis of data in qualitative research (Bryman & Bell, Business Research Methods 3/e, 2011) and is a well-established principal. Ritchie and Spencer (Ritchie & Spencer, 1994) detail out a 5 step **"Framework Analysis"** process for analysis of qualitative data for applied policy research, which aligns perfectly to the requirements of this research. The 5 step Framework Analysis is described and represented in the Figure 4-7 below.

- Familiarization: essentially involves the immersion in the data to identify recurrent themes and list key ideas.
- Identifying a Thematic Framework: involves identifying 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: is the approach to labelling data into manageable chunks for subsequent retrieval and exploration
- Charting: involves building the big picture view from the themes identified and involved abstraction and synthesis of the data gathered.

- 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 original intent of the study.

Figure 4-7: Ritchie and Spencer Framework Analysis Source: (Ritchie & Spencer, 1994)

4.8.5 RESEARCH DESIGN OBJECTIVE 1: SUMMARY

The summary of the research design to address objective 1 is captured in the Table 4-2 below. It highlights the execution approach and choices made at various points in the qualitative research sequence advocated by Bryman and Bell and provides a bird's eye view of the entire research design.

	Bryman and Bell's Sequence of steps in Qualitative Research	Execution Approach used in this research	Choices made in this research
1	General Research Question		
2	Selecting relevant site(s) and subjects	**Sampling**: Purposive, Non probabilistic Sampling. **Sample Size**: Theoretical Saturation	CIO's, CISO's, Service providers and Policy Makers in the Indian power sector and security domains.
3	Collection of relevant data	In-depth **semi-structured interviews** with a pre-defined **Interview Protocol**	

	Bryman and Bell's Sequence of steps in Qualitative Research	Execution Approach used in this research	Choices made in this research
4	Interpretation of Data	Ritchie & Spencer **Framework Analysis**	Leveraging Atlas TI for coding, formulating of themes, charting and interpreting.
5	Conceptual and theoretical work	Focus on identifying the cyber security challenge in the power sector	
6	Writing up findings / conclusions	To address Research Objective 1	i) Cyber security challenges in the Indian Power sector. ii) Final Set of Variables for as input for Research objective 2

Table 4-2: Execution Approach and Choices in the research to address Objective 1

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. Quantitative methods focus on objective measurements and statistical analysis of data collected using computational techniques. It focuses on gathering numerical data and generalizing it across groups of people or to explain a particular phenomenon (Babbie, 2010).

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

Table 4-3: Objective 2- Choices in this research

Bryman and Bell propose a multi-stage process to address quantitative research (Bryman & Bell, Business Research Methods 3/e, 2011) as shown in 4-8 below. The hypothesis for the research flows from the evaluation of the theory or the literature review. In some cases it is likely that in the place of the hypothesis, the theory acts loosely as a set of concerns in relation to the hypothesis.

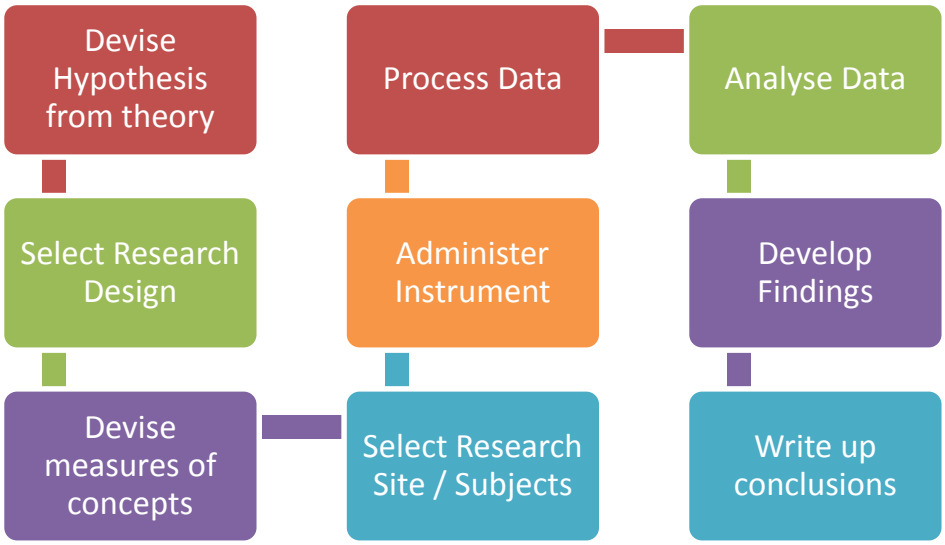

Figure 4-8: Quantitative Research Methods Adapted from (Bryman & Bell, Business Research Methods 3/e, 2011)

4.9.1 SELECT RESEARCH DESIGN

There are a number of choices of Research design in quantitative research – Experiment, Quasi-Experiment, Cross-Sectional Design and Longitudinal Design etc. The **Cross-Sectional Design** entails the collection of quantitative and quantifiable data at a single point in time of two or more variables which are then examined to detect patterns of association. **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 causality

4.9.2 DEVISE MEASURES OF CONCEPTS

Concepts are the building blocks of theory around which business research is conducted. "Concepts are categories for the organization of ideas and

observation" { (Bulmer, 1984) as cited in (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 the procedure of assigning numerical scores to various degrees of attitude or opinion or other concepts. The scale is continuum consisting of the highest point and lowest point with multiple intermediate points between the two extremes (Kothari C. R., 2013).

4.9.2.1 CHOICE OF SCALE – LIKERT-TYPE SCALE

Likert-type scales are developed using item analysis approach. The scale consist of a number of statements which express a favourable or unfavourable attitude towards a 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 are asked to agree or disagree with statement on a 5 point scale with varying degrees of agreement or disagreement. The Likert scale is shown in Figure 4-9 below.

The Likert-type scale has a number of advantages – it is relatively easy to construct, 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. (Kothari C. R., 2013).

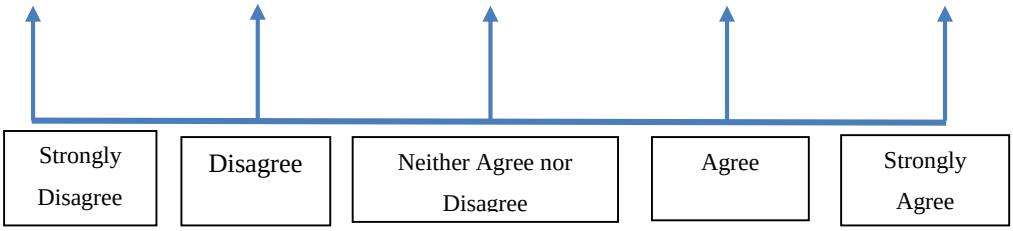

Figure 4-9: Likert-type Scale

The variables determined from the qualitative analysis as part of research design one formed the input for the Likert-type scale.

4.9.2.2 TESTING THE INSTRUMENT

i) 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.

ii) Reliability

Reliability refers to the consistency of a measure of a concept (Bryman & Bell, Business Research Methods 3/e, 2011). Reliability of an instrument can be 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). Schutte et al. suggest that as a "rule of thumb" a Cronbach's alpha score of 0.7 or above is deemed as an acceptable score (Schutte, Toppinnen, Kalimo, & Schaufeli, 2000).

iii) 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 cyber security domain and in the Indian power sector to establish the face validity of the instrument

4.9.3 SELECTION OF RESEARCH SITE (S) 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 electricity and cyber security domain, academics, CIO's, CEO's , service providers and electric city equipment providers. From within the power sector, the selection of people was taken from across the entire value chain from generation, transmission and distribution domains.

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 selected using random selection so that each unit in the population has a known chance of being selected. Probability sample are assumed to be representative sample. The popularity of probability sample stems from the fact that it is possible to make inferences or generalized the findings on the population from the information gathered from a random sample drawn from the same population. (Bryman & Bell, Business Research Methods 3/e, 2011).

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

- Policy Makers / Academicians / Think-tanks
- Members of the Indian Power Industry
- Service providers / System Integrators from Power sector and Security service provider

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:

i) **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 key role in cyber security of the power sector India. Over 1240 respondents across the three strata were identified as part of the sampling frame.

ii) **Sampling Element** - As the survey was aimed to elicit feedback on cyber security for the Indian Power Sector, the sampling element was defined as the people who were engaged in policy decision making, the middle or senior management in the Indian power sector or service providers.

iii) **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)

$$n = \frac{N}{1 + N.e^2}$$

Where n = Sample Size needed

N = Size of the Population

e = Levels of Precision

Applying the Yamane, formula for a population (N) size of 1000, and a precision (e) of +/- 5% would result in sample size (n) of 286 and a size of 169 for a precision level of +/- 7%.

An alternative approach to sample size determination is provided by Malhotra & Dash who suggests norm of 5 to 8 respondents per variable for factor analysis (Malhotra & Dash, 2011).

There are two broad schools of thought on recommendation of for the minimum acceptable sample size for factor analysis. The first is based on the population or the absolute number of cases (*N*), while the other focusses on the subject to variable ratio. Zhao in his review of the recommendation of sample size compiles the different recommendation by various researchers which is discussed below.

i) Sample size based on absolute size N

- Rule of 100:
  A number of researchers suggest that the no sample should not be below 100 even if the number of variables is less than 20. { (Gorsuch, 1983), (Kline, 1979) and (MacCullum , Widaman, Zhang, & Hong, 1999) as cited in (Zhao, 2009)}.
- Rule of 150:
  Hutcheson and Sofroniou suggests a sample size of between 150 and 300 and lean towards 150 when there are a few highly correlated variables { (Hutcheson, 1999) as cited in (Zhao, 2009)}.
- Significance rule:
  Lawley and Maxwell propose that sample size should be 51

more than the number of variables, to support chi-square testing (Lawley & Maxwell, 1972) as cited in (Zhao, 2009)}.

ii) Sample size based on Subject to Variable ratio

- Ratio of between 3 and 6

  Cattell recommends that the sample size should be between 3 and 6 times the number of variables. { (Cattell, 1978) as cited in (Zhao, 2009)}
- Ratio of 10:1

  A number of researchers including Everitt, and Kunce, Cook & Miller amongst others recommend a sample of 10 times the number of variable { (Everitt, 1975), (Kunce, Cook, & Miller, 1975) as cited in (Zhao, 2009)}
- Ratio of 20:1

  Hair et al. recommend that the sample size be at least 20 times the number of variable { (Hair, Anderson, Tatham, & Black, 1995) as cited in (Zhao, 2009)}

Bartlett's test of sphericity tests the hypothesis that the correlation matrix is an identity matrix or that the 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.).

The KMO measure also aims to establish the adequacy of the co-relation but uses a different approach. The KMO index uses the partial correlation to measure the relation between two variables by removing the effect of the remaining variables. The KMO index compares the values of correlations between variables and those of the partial correlations. 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 ‘marvellous’, while 0.80s would be ‘meritorious’, 0.70s ‘middling’, 0.60s ‘mediocre’, and below .5 ‘unacceptable’ (Dziuban & Shirkey, 1974).

With a variable size of 20, it would suggest a sample size of between 100 and 200 based on the various research papers. Given the wide range of opinion on the sampling size, this research adopts the **Bartlett’s test of sphericity** and **Kaiser-Mayer-Olkin (KMO)** measure of sampling adequacy to establish the adequacy of the co-relation matrices for factor analysis. The sample size of 172 respondents was used in this research.

4.9.6 ADMINISTER THE INSTRUMENT

The questionnaire was divided into six sections – section 1 through 6 with groups of questions aligned to a similar domain. The last section of the questionnaire 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 cyber security 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) (explained in the subsequent section) and using Amos software for analysis for generating the Confirmatory Factor Analysis.

4.9.8 ANALYSE THE 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 4-10 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 smaller loadings on other factors. In EFA the factors are derived from statistical results not from a-priori 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).

Confirmatory Factor Analysis (CFA) is a multivariate statistical technique that is similar to EFA and is also used to test how well the measured variables represent the number of constructs. There is however, an underlying or philosphical difference, in CFA the researcher uses the theory or a-priori knowledge to postulate the relationship between the construct or factor and the variable.

Structure Equation Modelling (SEM) is then applied to test the the extent which the researcher's a-priori pattern or assumptions of factor loading represent the actual data. CFA is a tool that is used to confirm or reject the measurement theory (Statistics Solution, 2013).

James Gaskin, suggests that CFA is the next step after the exploratory factor analysis to determine the factor structure. The EFA explains how the variables relate and group based on inter-variable correlations, while the CFA confirms the factor structure extracted in the EFA (Gaskin , Confirmatory Factor Analysis, 2012). He goes on to postulate that establishing reliability and validity is of utmost importance and is a pre-requisite when using CFA, because if the factors do not demonstrate adequate validity and reliability, it is meaningless to test a causal model.

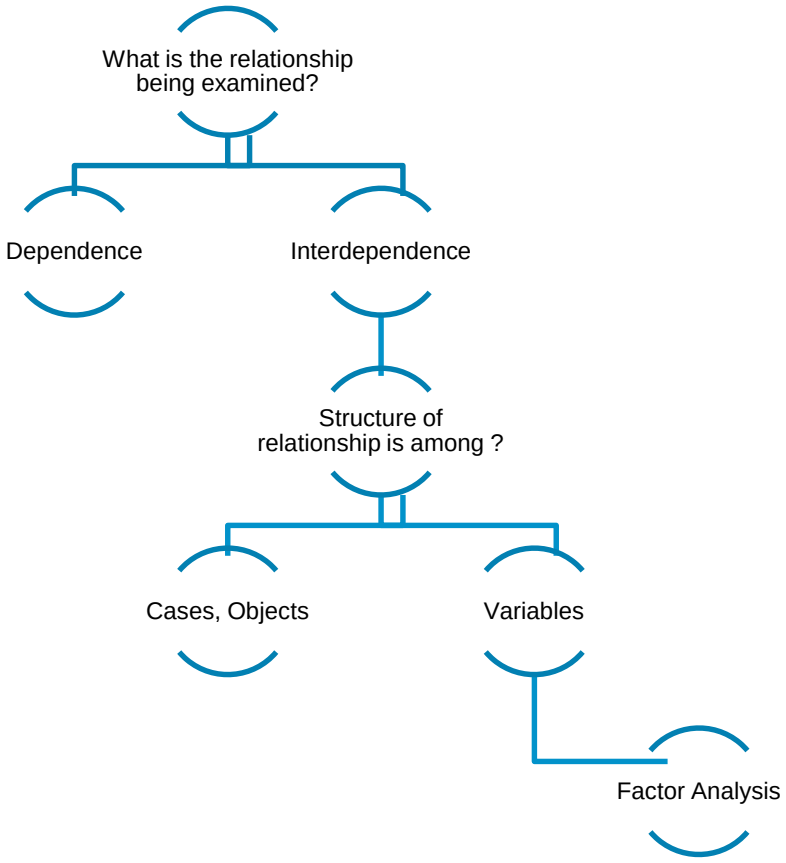

Figure 4-10: Classification of Multivariate Techniques

i) Composite Reliability (CR)

The Composite reliability is a measure of the overall reliability of a collection of heterogeneous but similar items, and differs from the reliability of individual items that is measures using Cronbach's alpha discussed earlier.

ii) Construct Validity

The previous section referred to the concept facevalidity, There are two other main measures of validity – **Convergent validity** and **Discriminant validity**, that together constitue **Construct validity**. Construct validity is "the degree to which a test measures what it claims, or purports, to be measuring" (Messick, 1980).

A measure of constructs that theoretically should be related to each other, are observed to be related to each other is deemed to posess **Convergent validity.** While measures of constructs that theoretically should not be related to each other are observed to not be related to each other is deemed to possess **Discriminant validity.**

iii) **Thresholds**

Hair et al. provide the thresholds for establishing reliability and convergent and discriminant validity { (Hair, Black, Babin , & Anderson, 2010) as cited in (Gaskin , Confirmatory Factor Analysis, 2012)} The theshold values are provided in the Table 4-4 below.

Measure	Threshold Value
Composite Reliability (CR)	• CR > 0.7
Convergent Validity	• Average Variance Extracted or AVE > 0.5
Discriminant Validity	• Maximum Shared Variance or MSV < AVE • Average Shared Variance < AVE • Square root of AVE greater than inter-construct correlations.

Table 4-4: Reliability and Validity Thresholds Source :{ (Hair, Black, Babin , & Anderson, 2010) as cited in (Gaskin , Confirmatory Factor Analysis, 2012)}

Malhotra and Dash (Malhotra & Dash, 2011) suggest that "AVE is a more conservative measure than CR. On the basis of CR alone, the researcher may conclude that the convergent validity of the construct is adequate, even though more than 50% of the variance is due to error."

iv) Evaluating Model Fit

Model fit refers to how well the proposed model explains the correlations between variables in the dataset. If all the 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 significant "discrepancy" between the correlations proposed and the correlations observed, it leads to a poor model fit, or the proposed model does not "fit" the observed or "estimated" model. Hu and Bentler { (Hu & Bentler, 1999) as cited in (Gaskin , Confirmatory Factor Analysis, 2012)} have identified a number of paratmeters to estimate the **Goodness of Fit** (GFI).

Measure	Threshold Value
Chi-square / df (cmin / df)	• < 3 Good, < 5 Permissible
p- Value for the model	• > 0.05
CFI (Compartive Fit Index)	• > 0.95 great; > 0.9 traditional; > 0.8 sometimes permissible
GFI (Goodness of Fit Index)	• > 0.95
AGFI (Adjusted Goodness of Fit Index)	• > 0.80
SRMR (Standardized Root Mean Square Residual)	• < 0.09
RMSEA (Root Mean Square Error of Approximation)	• < 0.05 good; 0.05 – 0.1 moderate; >.10 bad
PCLOSE	• > 0.05

Table 4-5: Indices of Fit Source :{ (Hu & Bentler, 1999) as cited in (Gaskin , Confirmatory Factor Analysis, 2012)}

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 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.

4.9.11 SUMMARY RESEARCH DESIGN: OBJECTIVE 2

The entire research design to address objective 2 is captured in the Table 4-6 below. It highlights the execution approach and choices made at various points in the quantitative research sequence advocated by Bryman and Bell and provides a bird's eye view of the entire research design for objective 2.

	Bryman and Bell's Sequence of steps in Qualitative 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 Measures of concepts	Choice of Scale: **Likert-type Scale** Testing the Instrument: **Pilot** **Reliability** **Validity**	5 point Likert-type scale Cronbach's Alpha Face Validity
4	Selecting relevant site(s) and subjects	**Sampling**: Probability sampling. Stratified random sample **Sample Size**: Validated with Bartlett's test of sphericity and KMO measure of sampling adequacy	CIO's, CISO's, Service providers and Policy Makers in the Indian power sector and security domains.
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

	Bryman and Bell's Sequence of steps in Qualitative Research	Execution Approach used in this research	Choices made in this research
7	Analyze the Data	Exploratory Factor analysis for data reduction and identifying the factors Establish Composite Reliability Convergent Validity Discriminant Validity Goodness of Fit Indicator Confirmatory Factor Analysis to establish the significance	Identify the factors that enhance cyber security in the Indian power sector 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 cyber security in the Power sector.
8	Writing up findings / conclusions	To address Research Objective 2	Factors that enhance cyber security in the Indian power sector and their significance.

Table 4-6: Execution Approach and Choices in the research to address Objective 2

4.10 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 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 - familiarization, identification of a thematic framework, indexing, charting and Mapping & Interpretation. Atlas TI was the tool of choice to process the data for analysis. Qualitative analysis helped answer the first research question on the cyber security challenges in the Indian power sector.

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 cyber security in the Indian power sector 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 first section of the data analysis focusses on the qualitative aspects that focusses on understanding the cyber security challenges in the Indian Power Sector and output of the analysis helps identify the variables for the factor analysis. The second section answers the question on the factors that enhance cyber security in the Indian Power Sector using Exploratory Factor Analysis and understand their significance with Confirmatory Factor Analysis.

5.2 QUALITATIVE DATA ANALYSIS: OBJECTIVE 1

Purposive sampling or judgmental sampling is employed in this research. The CIO / COO / GMs of Power Companies, Policy Makers in the Government of India from Cert-In, NTRO, Office of NSA and leading Suppliers across both Power Sector and Security Provider were handpicked based on their expertise and knowledge in the sector. In depth interview was conducted by using the Interview Protocol attached in

APPENDIX A: Interview Protocol.

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

5.2.1 DATA INTERPRETATION

Ritchie & Spencer's Framework Analysis has five components namely: Familiarization, Identifying a Thematic Framework, Indexing, Charting, Mapping and Interpretation, as detailed out in the preceding chapter. The transcripts were reviewed 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 next section.

5.2.2 THEMATIC FRAMEWORK

A number of common themes emerged from the in-depth interviews. These include reference to R-APDRP as a stimulus for investment in the Power Sector, the investment in IT driving increased automation in the Indian Power Sector, poor security awareness, lack of executive ownership of cyber security, little or no information sharing and collaboration within the industry, need for data protection and a preference for normative or principle based regulation. The familiarization and identifying thematic framework is shown in Figure 5-1 below.

5.2.3 INDEXING

Coding and Indexing is the approach to labelling data into manageable chunks for subsequent retrieval and exploration. Atlas TI enabled us to break the drudgery of coding by automating a number of intermediate tasks. The sample screen shot of indexing using Atlas TI is captured in the Figure 5-2 below. The

codes that were identified are mapped back or "indexed" to the themes that emerged from the in-depth interview.

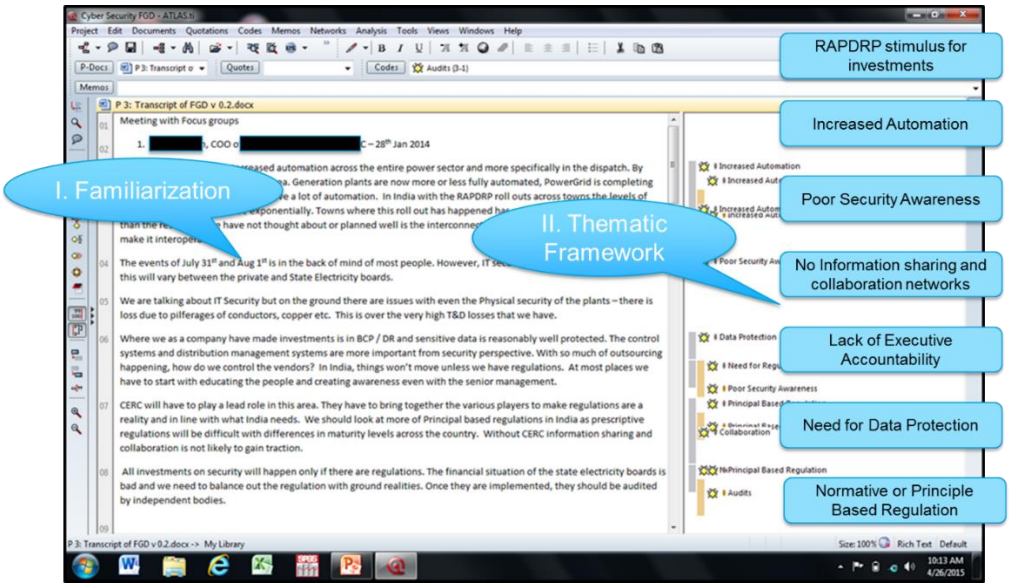

Figure 5-1: Familiarization and Thematic Framework

5.2.4 CHARTING AND 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 involves tying up of the expert opinion gathered 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 power sector and related constructs. The next section provides a background of the Indian power sector relevant to this research.

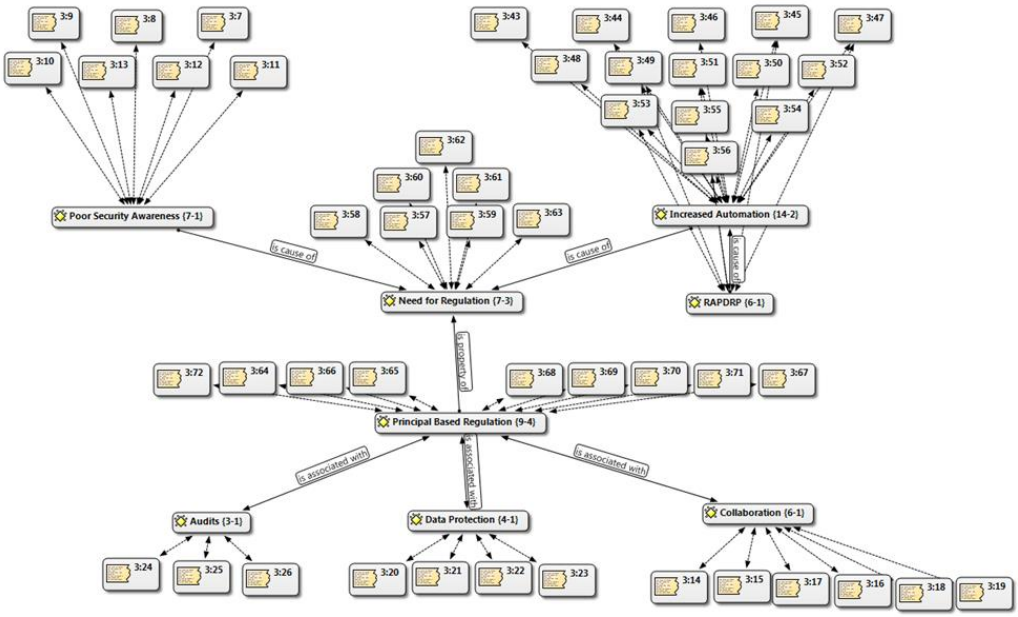

Figure 5-2: Indexing, charting and mapping using Atlas TI

5.2.5.1 BACKGROUND

India has an installed power generation capacity of a little over 280,000 MW (Central Electricity Authority, 2015) from an installed capacity of just 1,362 MW (Indian Power Sector, n.d) at the time of independence. "Electricity" in India is a "Concurrent subject", subject to the jurisdiction of the Centre and the States. The planning at the national level and the regulatory framework in the Indian Electricity sector is governed by the Electricity (Supply) Act, 1948, amended in 1991 when the government of India initiated broad-based reforms. The 1998, Electricity Regulatory Commission Act, 1998, envisaged the creation of an independent regulator for the Power Sector, the Central Electricity Regulatory Commission at the national level (CERC) and the State Electricity Regulatory Commission (SERCs) at the State levels. The role of the CERC is to regulate the tariff of generating companies owned or controlled by the Central Government, when more than one state is involved, inter-state bulk sale of power, and to aid & advise the Central Government in formulation of tariff

policy. The SERC regulates the tariff for electricity wholesale bulk, grid or retail, regulate transmission and distribution, improve efficiency and promote competition, efficiency and economy in the activities of the electricity industries etc. Subsequently, as and when each State Government notifies, other regulatory functions would also be assigned to SERCs. The Electricity Laws (Amendment) Act, 1998 was passed with the objective to make transmission as a separate activity to provide for private investment and participation in the transmission sector. It provides for the setting up of Central and State Transmission utilities, to undertake transmission of energy through inter-state transmission system and discharge all functions of planning and coordination relating to transmission. The Power Grid Corporation of India Limited is the Central Transmission Utility. Similarly the State Transmission Utility undertakes transmission within the state boundaries (Indian Power Sector, n.d).

McKinsey & Co in their report on the Indian Power Sector ((McKinsey & Co, 2010) point out that India will have a potential peak deficit of 70 Giga Watt by 2017. The bane of the Indian Power Sector has been the un-remunerative tariff structure (Indian Power Sector, n.d) and very high Aggregate Technical and Commercial (AT&C) loss (Ministry of Power, Government of India, 2013). The precarious financial situations of the State Electricity Boards (SEBs) are well documented in numerous publications { (OECD, 2014), (Bajaj & Sharma, 2006)}. The accumulated losses of the distribution utilities in India stood at a mammoth 3.8 Lakh crores (approximately USD 59.3 Billion) (The Hindu Bureau, 2015) for the year ending Mar 2015.

The AT&C losses in India vary from as high as 73% in states like Jammu & Kashmir to 14% in Kerala (Ministry of Power, Government of India, 2013) with the national average pegged at over 30% (Sarkar, 2014). The Restructured-Accelerated Power Development and Reforms Programme (R-APDRP) is the Government of India's flagship program to reduce the AT&C losses in the country and to improve the power distribution sector of state utilities. The R-

APDRPP scheme is taken up in town with a population more than 30,000 (10,000 for special category States) as per the population survey of 2001 (Ministry of Power, Government of India, 2013). The scheme has two parts

- Part-A for establishing IT enabled system for energy accounting / auditing and Supervisory Control and Data Acquisition (SCADA) for big cities (Population of 400, 000+ & Energy Input of 350 MU per annum) and adoption of IT enabled infrastructure for management information systems, billing collection and addressing customer grievances.
- Part-B for up-gradation, strengthening and augmentation of strengthening the electrical infrastructure in towns.

In the XI plan period, as of ending Mar 2013, projects worth Rs. 32,323.70 crores (approximately USD 505 Million @ Rs. 64 / USD) were sanctioned by the Government of India covering over 2500 towns across both Part-A and B (Ministry of Power, Government of India, 2013). The Government of India has announced the intention to extend the RAPDRP program into XII and XIII plan period and committed a budget outlay of another Rs. 22,727 crores (approximately USD 355 Million) (Government of India, Ministry of Power, 2008). Apart from the background on the power sector, is the characteristics of a principle based regulations that is distinct from a rule based regulation.

The choice of regulatory intervention or mandate can be twofold:

- Prescriptive Regulations or Mandate a good example of this is the Payment Card Industry – Data Security Standards mandate on credit card protection
- Normative or Principle based regulations e.g. ISO 27001

Principles-based regulation implies moving away from a detailed and prescriptive rule, while relying more on high-level, broadly stated rules or Principles to set the standards by which regulated firms must conduct business

(Black, Hopper, & Band, 2007). Black et al. suggest that Principle based regulations exhibit three characteristics:

- A preference to road-based standards instead of detailed rules
- Outcomes-based regulation
- Increased senior management responsibility

The background data with the outcome of the in-depth interviews sets the stage for the interpretation.

The diversity in the Indian Power Sector and financial status of many of the operators were the overwhelming reason for the respondents to voice their preference for recommending a principle based regulation for the Indian Power Sector. This preference for a more broad based principle lead regulation meant the number of variables that were directly related to technology controls from the literature review was not considered relevant in the Indian context.

The increased IT adoption, driven by the R-APDRP program has delivered a number of benefits with a reduction in AT&C losses across nearly all the utilities in the country as per the report presented in the parliament by the Union Minister for Power (Government of India, Ministry of Power, 2015). There was universal recognition amongst the respondents on R-APDRP as the single biggest stimulus to IT investment in the Indian Power Sector. Every single respondent brought up R-APDRP as the driver for increased IT adoption. There are a number of IT lead initiatives that are undertaken with the funding from the R-APDRP Program and examples of how IT adoption has improved significantly in the metering, billing and collection space and increased adoption of SCADA / DMS or Distribution Management systems. The increased adoption of IT was noted as a definite positive across the spectrum of respondents.

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

The CIO of one of the utilities pointed out that Tata Power, New Delhi was the first utility provider that had voluntarily sought and acquired accreditation to the ISO 27001 security standard as late as in 2011. While the respondents highlighted that integrated management system manual that is used in many organizations are usually aligned to ISO 27001 amongst others, not too many other players were accredited to this or similar standard. Analysis of secondary data showed Reliance Infrastructure, the utility responsible for Mumbai and POSOCO the wholly owned subsidiary of Powergrid Corporation, the central transmission utility are also accredited to ISO 27001. It is likely that more players are accredited to a security standard, this suggests that cyber security is probably not top of the mind recall within the industry. The expectation was that the system integrators and vendors would bake in security when the solution was being designed and deployed. This view is substantiated with examples of ISO 27001 being a mandatory requirement for the ICT vendors.

The respondents brought out that barring a few organizations, the role of a CISO or a similar role was not well established in the Indian Power Sector. The role of security executive leadership was assumed to be part of the IT team or subsumed with the CIO organization. This point of view can be substantiated with secondary data points from the field, for example it is only as recently as Oct 2015 that BESCOM, the Bangalore Electricity Supply Company, notified the board resolution to create a separate cadre for Information Technology and creation of the position of a General Manager for Information security (Bangalore Electricity Supply Company, 2015). The downside of this has meant that there is very little appreciation of the cyber threat at the board level. A common theme across the respondents was the minimal awareness both at the executive level and across the rank and file when it comes to cyber security controls beyond what is reported in the popular press.

Given the financial situation and the technology capabilities with the SEBs and mixed success with reforms in the power sector historically, an emerging view was that success with voluntary compliance is likely to be quite low in the distribution segment, while the success could be higher with the central

generation and transmission organization. The way forward to increased adoption of cyber security process is to make it a mandatory requirement driven by the CERC. This could take the form of guidelines or mandatory requirements.

The exception to the trend on low security awareness was the protection against financial threats and Data security. The respondents pointed that this Data security was almost synonymous with protection of financial transaction. There was a recognition that with an increased adoption of the e-commerce and internet for electronic bill presentation and payment services by the SEBs, increased the threat exposure and therefore for the stronger data privacy requirements.

R-APDRP has brought in IT intervention in two other areas – Control Automation and Asset base-lining. This was reflected in the respondents view as areas to be addressed from a cyber-security perspective. The respondents called out the need for identification and protection of critical cyber assets and periodic review of the security configurations of these assets.

The Ministry of Power, has mandated the three sector specific CERTs in the Power sector. - CERT- Thermal, CERT- Hydro and CERT- Transmission to promote information sharing and collaboration (Government of India, Northern Regional Power Committee, 2014), the need for information sharing and collaboration was called out by the respondents as well.

5.3 ANSWER TO THE RESEARCH QUESTION 1 (RQ)

The summary of the outcome of the qualitative analysis to identify the challenges in the Indian Power Sector is described in the Figure 5-4 below.

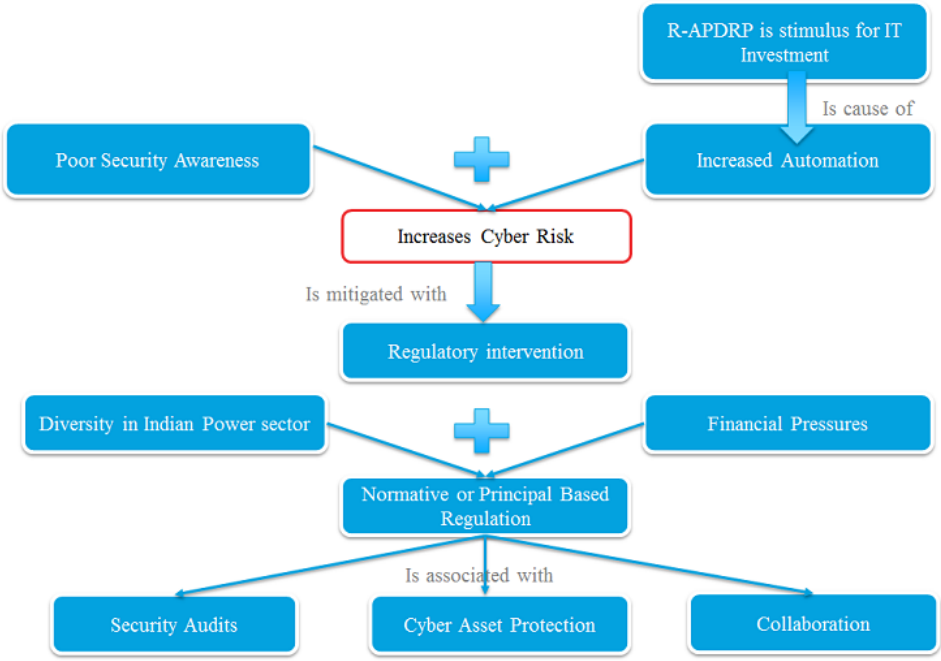

Figure 5-3: Summary of the Qualitative Analysis

The increased IT adoption, driven by the R-APDRP program has delivered a number of benefits with a reduction in AT&C losses across nearly all the utilities in the country. There is however, very little appreciation of the risks or exposure to cyber security threats which comes along with the increased adoption of IT both among the executives and in the rank and file of the power sector. A majority of the organization do not have designated CxO level executive responsible for cyber-security and the security function is usually subsumed within the IT organization. Given the diversity and the financial status of the players in the Indian Power Sector, a principle based regulatory intervention lead by CERC emerged as a preferred choice to enhance cyber security in the power sector. A principle 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 the first research question.

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 28 variables that emerged from the literature review was narrowed down to 20 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.

Cronbach's alpha, (which is defined in detailed in the previous chapter) was used to measure the internal reliability.

The Cronbach's alpha score of 0.76, 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.

The Cronbach's alpha test was repeated once the entire data collection was completed before the factor analysis. This showed an improved Cronbach's alpha score of 0.86 as shown in Table 5-2 below.

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	N of Items
.760	20

Table 5-1: Cronbach's Alpha score based on first 30 respondents

Case Processing Summary

		N	%
Cases	Valid	172	100.0
	Excluded[a]	0	.0
	Total	172	100.0

a. List wise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.855	20

Table 5-2: Cronbach's Alpha score with all the respondents

5.4.2 KMO AND BARTLETT'S TEST

The Kaiser-Meyer-Olkin (KMO) index is measure of sampling adequacy and Bartlett's Test of Sphericity tests the hypothesis that the variables form an identity matrix with no co-relation between them.

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.806
Bartlett's Test of Sphericity	Approx. Chi-Square	1.098E3
	df	190
	Sig.	.000

Table 5-3: KMO and Bartlett's Test

Interpreting KMO Score
0.9+ -
0.8 – 0.89 - Meritorious
0.7 – 0.79
0.6 – 0.69
0.5 - 0.59
< 0.5 - Unacceptable

Table 5-4: Interpreting the KMO Score

The KMO score of .809 is deemed as meritorious and confirms the sampling adequacy of the research (Dziuban & Shirkey, 1974).

Bartlett's test of sphericity tests the hypothesis that the variable are independent. We are able to reject the hypothesis as the significance is .000. The data set is now ready to proceed to factor analysis.

5.5 EXPLORATORY FACTOR ANALYSIS (EFA) RESULT

EFA is statistical technique that deals with multiple variables. EFA focusses on identifying a structure or factor that explains the inter-relationship amongst a set of observed variables. It is thus a data reduction technique that where a number of observed variables are "reduced" or "grouped" into a smaller number of factor. EFA transforms the correlations in the set of observed variables into a smaller number of underlying factors that still retains the essential information about the linear interrelationships among the original variables (Lyytinen & Gaskin, 2014). There are three decision points in factor analysis that would need to be considered. The decision points are listed below and discussed in the subsequent sections (Costello & Osborne, 2005)

- Extraction - Component vs. Factor Extraction,
- Number of Factors to Retain
- Rotation: Orthogonal vs. Oblique

5.5.1 EXTRACTION

There are a number of different approaches to Extraction and Costello & Osborne, highlight the challenge 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 nomenclature 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).

Principal Component Analysis considers all of the available variables and seeks a linear combination of variables such that maximum variance is extracted and this process is repeated till the factors are extracted. It results in an orthogonal array of uncorrelated factors (Lyytinen & Gaskin, 2014).

Common Factor Analysis or Principal Axis Factoring considers only the common variance. It seeks to identify the least number of factors that can account for the common variance or correlation of a set of variables.

There are multiple schools of thought that favour 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 (Costello & Osborne, 2005). This research uses the Principal Component Analysis for Extraction.

5.5.2 NUMBER OF FACTORS TO RETAIN

The next decision point after extraction is to decide on the number of factors to retain. Costello & Osborne suggest that 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 fewer than three 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.
- Examining the scree plot of Eigenvalues for the break point in data where the curve flattens out. The number of data points above the "break" is the number of 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 factors that are uncorrelated while oblique rotation methods allow the factors to correlate.

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

A communality is measure to which an item correlates with all other items. Higher the communality, better the correlation. When the communalities for a particular variable are low (< 0.4), it would imply that the variable would struggle to load significantly on any factor (Gaskin, Exploratory Factor Analysis, 2012). The Table 5-5 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.

Communalities

	Initial	Extraction
IS&C_1	1.000	.565
IS&C_2	1.000	.738
IS&C_3	1.000	.759
SecA_1	1.000	.450
SecA_2	1.000	.667
SecA_3	1.000	.554
CCPA_1	1.000	.644
CCPA_2	1.000	.523
CCPA_3	1.000	.735
PnO_1	1.000	.570
PnO_2	1.000	.666
PnO_3	1.000	.728
DP_1	1.000	.553
DP_2	1.000	.518
DP_3	1.000	.595
DP_4	1.000	.690
DP_5	1.000	.678
RiskA_1	1.000	.598
RiskA_2	1.000	.738
RiskA_3	1.000	.690

Extraction Method: Principal Component Analysis.

Table 5-5: Communalities

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 six factors where the Eigenvalues is of 1 or more represent 63.3% of the total variance in the 20 variables.

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	5.686	28.428	28.428	5.686	28.428	28.428	2.633	13.163	13.163
2	1.778	8.889	37.317	1.778	8.889	37.317	2.177	10.887	24.050
3	1.641	8.203	45.520	1.641	8.203	45.520	2.075	10.373	34.423
4	1.405	7.025	52.545	1.405	7.025	52.545	1.970	9.851	44.274
5	1.115	5.573	58.118	1.115	5.573	58.118	1.953	9.765	54.038
6	1.036	5.179	63.297	1.036	5.179	63.297	1.852	9.258	63.297
7	.889	4.447	67.744						
8	.779	3.896	71.640						
9	.759	3.794	75.433						
10	.668	3.338	78.771						
11	.596	2.979	81.750						
12	.544	2.722	84.472						
13	.498	2.491	86.963						
14	.480	2.400	89.362						
15	.451	2.253	91.615						
16	.430	2.148	93.763						
17	.379	1.897	95.659						
18	.353	1.766	97.426						
19	.305	1.525	98.950						
20	.210	1.050	100.000						

Extraction Method: Principal Component Analysis.

Table 5-6: Factor Analysis: Six Factors explain 63.3% of the variance

5.7 ROTATED COMPONENT MATRIX

The rotated component in Table 5-7 shows the 20 variables loading onto six 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 discussed in the previous section of the chapter.

5.8 ANSWER TO THE FIRST PART OF CENTRAL RESEARCH QUESTION – CRQ

The factors that emerged from the Exploratory Factor Analysis answers the first part of the CRQ. The six factors that enhance cyber security in the Indian Power Sector are shown in Figure 5-4 below.

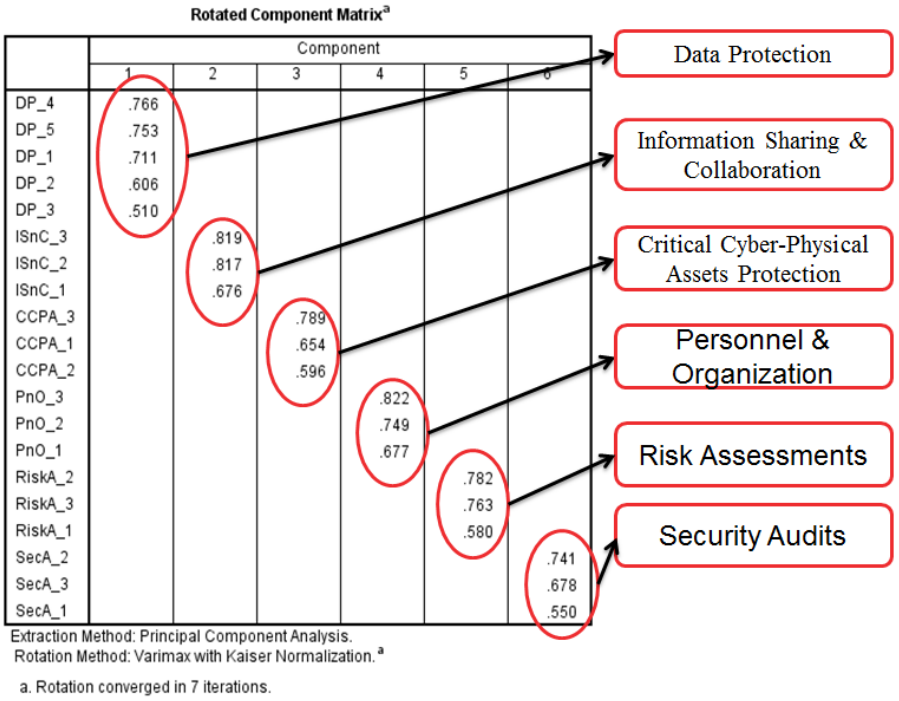

Table 5-7: Rotated Component Matrix

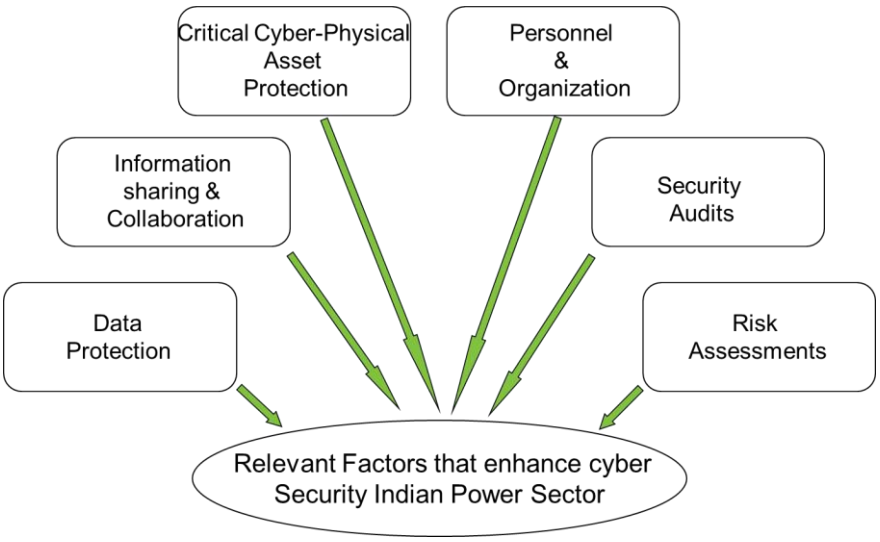

Figure 5-4: Factors that enhance cyber security in the Indian Power Sector

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 latents 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 (Schreiber, Nora, Stage, Barlow, & King, 2006) in their review paper provide a structure and approach to reporting on CFA / SEM research. 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 display 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 (Schreiber, Nora, Stage, Barlow, & King, 2006) survey identifies a number of different threshold metrics 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 modified and reanalysed, 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 preceding chapters on Literature review and research design. The CRQ is "What are the relevant factors that enhance cyber security and their significance in the Indian Power Sector?" The factors identified using EFA and CFA is proposed to establish their significance.

5.9.2 THE RATIONALE FOR THE CFA

The rationale and approach to CFA has been detailed out in the previous chapter on Research Design. CFA is the next step after the Exploratory Factor Analysis to determine the factor structure. The EFA explains how the variables relate and group based on inter-variable correlations, while the CFA confirms the factor structure extracted in the EFA (Gaskin , Confirmatory Factor Analysis, 2012).

5.10 STRUCTURAL FRAMEWORK FOR THE MEASUREMENT MODEL

The theoretical grounding for the research flows from the gaps in the literature review that established the lack of a domain specific cyber security mandate for the Indian Power Sector. The analysis of the global practices provided the initial set of variables that could be consider for evaluation for the Indian context. The qualitative analysis helped validate the challenges in the Indian Power Sector

and narrow down the variables relevant to the Indian Power Sector. The 20 variables were reduced to six factors as explained in the EFA sections in this chapter that provides the structural framework for the measurement model.

The next three requirements – appropriate tables and figures, the path models and inferences are the focus of the subsequent sections of this chapter. The approach to sample size has been discussed extensively in the preceding chapter on research design and adequacy of sample size {(n) = 172)} established in the preceding section of this chapter. The software used for CFA in this research was Amos (v 23) and stat tools package by James Gaskin (Gaskin, Stattools Package, 2012) for calculation of model fit indices.

5.11 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 to test for common method bias. This is done by constraining the number of factors extracted 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).

5.11.1 HARMAN'S SINGLE FACTOR TEST

The result of the Harman's single factor test shows that cumulative loading accounts for only 28.4% 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.

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	5.686	28.428	28.428	5.686	28.428	28.428
2	1.778	8.889	37.317			
3	1.641	8.203	45.520			
4	1.405	7.025	52.545			
5	1.115	5.573	58.118			
6	1.026	5.129	63.247			

Table 5-8: Harman's Single factor test result

5.12 PATH MODELS - CONSTITUENTS

In the path model or the Structural Equation Diagram (SEM) diagram the variables or latents are shown as ellipses, the variables or indicators are depicted in rectangles and the error and residual terms in circles. The causal relations are shown as arrows and double-headed arrows are used to show correlations between indicators or between exogenous latents. Path coefficient values are placed on the arrows (Lyytinen & Gaskin, 2014).

Gaskin and Lyytinen identify various stages in building the structural equation modelling.

1. Defining Individual Constructs
2. Developing the Overall Measurement Model
3. Designing a Study to Produce Empirical Results
4. Assessing the Measurement Model Validity
5. Specifying the Structural Model
6. Assessing Structural Model Validity

CFA involves the first 4 stages and SEM would be stages 5 and 6. In this research we stop with first 4 stages as the objective of the research is establish the validity of the measurement model and test the significance.

5.13 INITIAL CFA PATH MODEL

The first path model in Amos was arrived at based on the rotated component matrix output of the EFA. The initial path model is show in Figure 5-5 below.

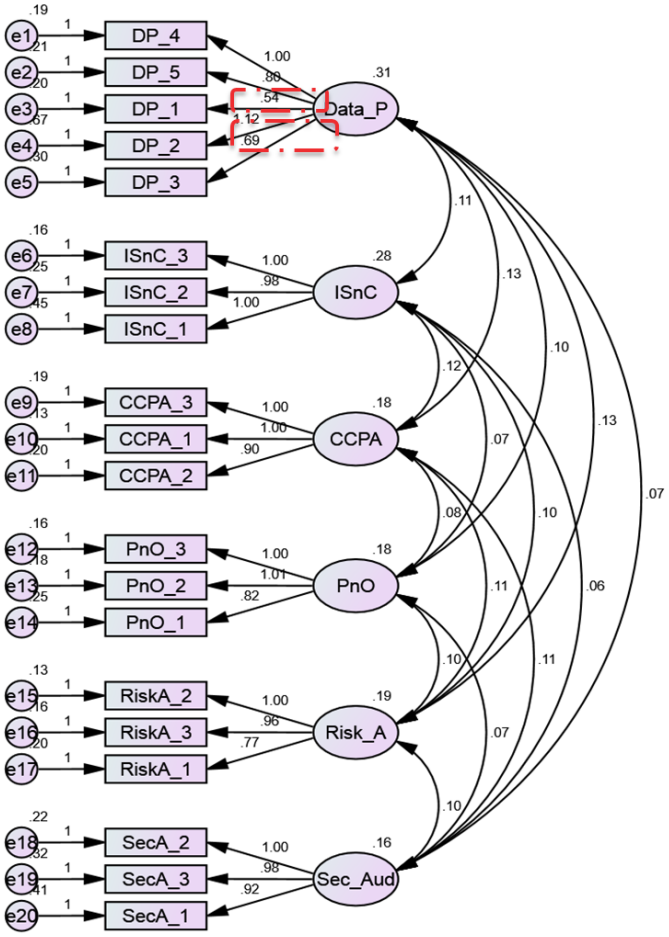

Figure 5-5: Initial CFA path model

The analysis of the path model shows a Reasonable model "Fit" with overall good loading of variables onto factors with all but two variables having a loading of 0.7 or greater. There is a low covariance between the factors. The next step is the evaluation of the Modification indices, the **Modification Indices**

(M.I.) are shown in Figure 5-6 below. The analysis of the M.I data set to a threshold value of 4 shows no large M.I scores that could cause concerns and also no covariance between residual errors.

			M.I.
e9	<-->	e17	5.86
e7	<-->	SecAud	5.428
e7	<-->	e17	8.204
e6	<-->	SecAud	7.844
e4	<-->	ISAC	4.888
e4	<-->	e17	4.698
e4	<-->	e9	10.214
e4	<-->	e7	10.914
e2	<-->	e7	7.764

Figure 5-6: Modification Indices of initial path model

The next step in CFA is the evaluation of model fit. The details of the criteria for evaluating model fit.

5.14 CRITERIA FOR EVALUATING MODEL FIT

As discussed in the previous chapter on research design, there is no one single universally accepted measure of model fit. In this research we use the Hu & Bentler's (Hu & Bentler, 1999) recommendation for evaluating model fit.

5.14.1 MODEL FIT THRESHOLD METRICS – INITIAL PATH MODEL

The metrics for the initial path model are captured in the Table 5-9 below. The analysis of the metrics show that the model meets 5 of the 6 metrics for good model fit and only the GFI score is below par.

Measure	Ideal Threshold	Actual
Chi-square/df* (cmin/df)	< 3 good;	1.386
CFI	> .95 great; > 0.9 traditional	.938
GFI	> 0.95	.897
AGFI	> 0.80	.86
RMSEA	< 0.05 good; 0.05 - 0.1 moderate;	.047
PCLOSE	> 0.05	.595
***df – Degree of Freedom**		

Table 5-9: Threshold metrics for initial path model

We look at the points of re-specification of the path model to improve model fit. The recommended approach to re-specification is articulated in the next section.

5.14.2 RE-SPECIFICATION OF LATENT VARIABLES OR MODEL FIT

David Kenny (Kenny, 2011) recommends multiple steps to improving the model fit or specification of the model. The approach adopted in this study is elaborated below.

i) Reduce large Modification indices

Modification indices MI, can be used to remediate discrepancies between the proposed and estimated model. Modification indices are

identified for covariance, and the first step is to co-vary error terms that are part of the same factor (Gaskin , Confirmatory Factor Analysis, 2012). M.I are quite low in this study and there is no co-variance of error terms possible to help improve the metrics.

ii) Drop variables with low factor loading

Identification of variables with low factor loading can help improve the model fit. There are two variables with low factor loading – Var DP_1 and Var DP_3 that load poorly (< 0.7) on the latent factor "Data Protection". These two variables can be dropped to validate if there is an improvement of model fit.

iii) Evaluate Discriminant validity to retain or drop factors
Discriminant validity tests can identify factors that can be dropped to improve model fit.

5.15 REVISED PATH MODEL – ITERATION 1

The revised path model after dropping the two variables at the end of the first iteration is shown in the Figure 5-7 "Revised Path Model Iteration 1" below and the threshold metrics for the Iteration 1 is captured provided in Table 5-10 (*df – degrees of freedom).

The review of the threshold metrics show that the dropping of the two variables have improved the threshold metrics from the initial path model but there is still scope for improvement. The evaluation of the discriminant validity scores is the next step to help identify further opportunities to improve the model fit.

Measure	Ideal Threshold	Actual
Chi-square/df* (cmin/df)	< 3 good;	1.424
CFI	> .95 great; > 0.9 traditional	0.94
GFI	> 0.95	0.90
AGFI	> 0.80	0.869
RMSEA	< 0.05 good; 0.05 - 0.1 moderate;	0.05
PCLOSE	> 0.05	0.493

Table 5-10: Threshold metrics for the revised path model - Iteration 1

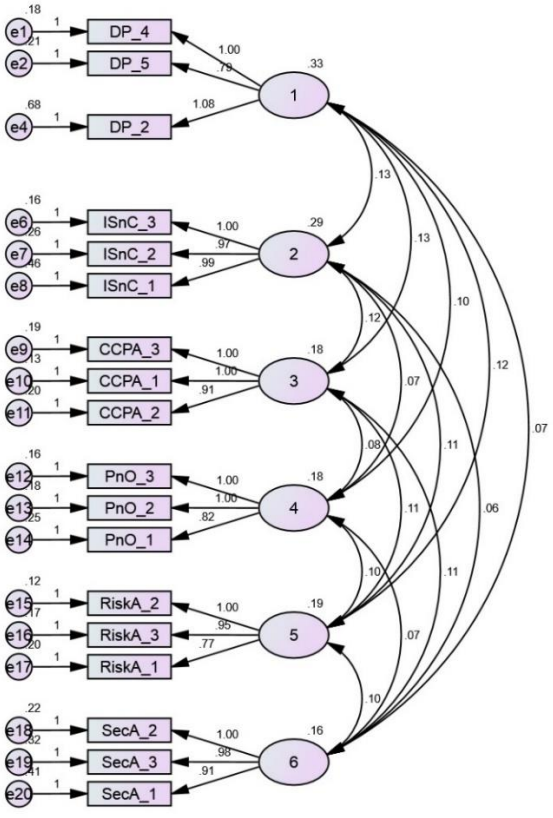

Figure 5-7: Revised Path Model Iteration 1

5.16 COMPOSITE RELIABILITY AND VALIDITY MEASURES

The Composite Reliability (CR), Average Variance Extracted (AVE), Maximum Shared Variance (MSV) and Average Shared Variance (ASV) scores for the model were calculated using James Gaskin's stat tool package (Gaskin, Stattools Package, 2012) and the results are captured in the Table 5-11 below. The perusal of data in the table shows that the all the variables except Risk assessments meet the requirements for composite reliability, convergent validity and discriminant validity. The threshold value for composite reliability, convergent validity and discriminant validity are provided in the previous chapter on research design.

	CR	AVE	MSV	ASV	SecAud	DP	ISAC	CCA	PnO	RiskA
SecAud	0.7	0.5	0.4	0.3	0.7					
DP	0.7	0.5	0.3	0.2	0.5	0.7				
ISAC	0.8	0.5	0.3	0.2	0.4	0.4	0.7			
CCA	0.7	0.5	0.4	0.3	0.6	0.5	0.5	0.7		
PnO	0.7	0.5	0.3	0.2	0.5	0.4	0.3	0.4	0.7	
RiskA	0.6	0.3	0.4	0.2	0.6	0.3	0.3	0.7	0.4	0.6

Table 5-11: Reliability and Validity metrics

A failure on the discriminant validity test would suggest that we can drop Risk Assessment as a factor and then create a fresh path model.

5.17 REVISED PATH MODEL - ITERATION 2

The latent factor- Risk Assessments was dropped and a third path model was defined. The output of the revised path model – Iteration 2 is shown in figure 5-8 below.

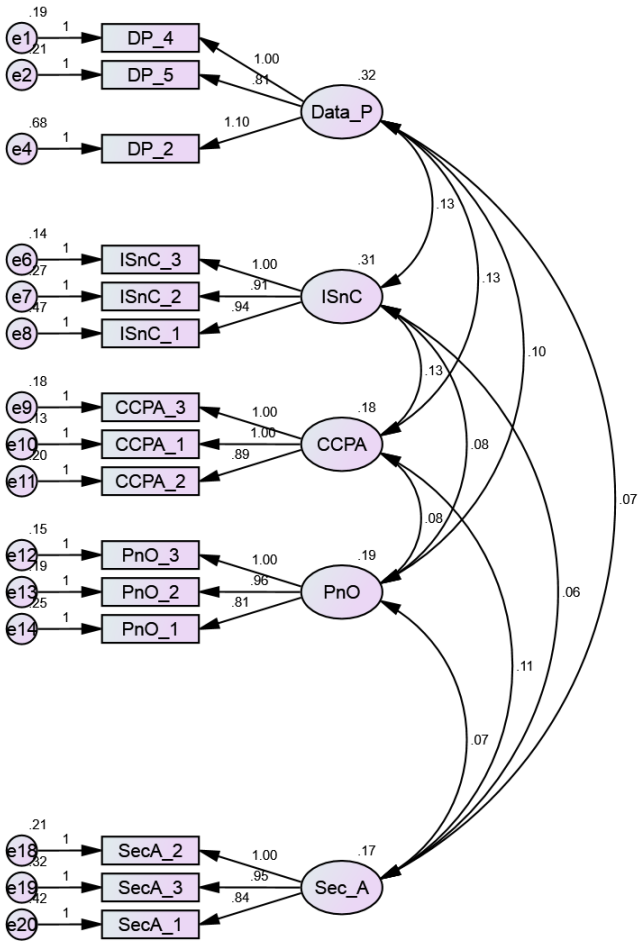

Figure 5-8: Path Model - Iteration 2

The revised reliability and validity metrics and model fit scores are captured in Table 5-12 and Table 5-13 respectively below. The review of the reliability and validity scores establish the composite reliability, convergent and discriminant validity of the revised path model.

	CR	AVE	MSV	ASV	PnO	DP	ISAC	CCA	SecAud
PnO	0.7	0.5	0.3	0.2	0.7				
DP	0.7	0.5	0.3	0.2	0.4	0.7			
ISAC	0.8	0.5	0.3	0.2	0.3	0.4	0.7		
CCA	0.7	0.5	0.4	0.3	0.4	0.5	0.5	0.7	
SecAud	0.7	0.5	0.4	0.3	0.5	0.5	0.4	0.6	0.7

Table 5-12: Iteration 2 Reliability and Validity score

Measure	Ideal Threshold	Actual
Chi-square/df* (cmin/df)	< 3 good;	1.46
CFI	> .95 great; > 0.9 traditional	0.95
GFI	> 0.95	0.92
AGFI	> 0.80	0.89
RMSEA	< 0.05 good; 0.05 - 0.1 moderate;	0.05
PCLOSE	> 0.05	0.42
***df – Degree of Freedom**		

Table 5-13: Threshold metrics - Iteration 2

The review of the table show that 5 of the 6 metrics meet the threshold metrics norm and the sixth measure GFI is at 0.92 as against a recommended Hu & Bentler's threshold of 0.95.

Traditionally an omnibus cut-off point of 0.90 has been recommended for the GFI. The more stringent 0.95 metric cut off was recommended by Miles and Shevlin { (Miles & Shevlin, 1998) as cited in (Hooper, Coughlan, & Mullen, 2008)}. Sharma et al point out that when there are a large number of degrees of freedom in comparison to sample size, the GFI has a downward bias (Sharma, Mukherjee, Kumar, & Dillon, 2005) as cited in (Hooper, Coughlan, & Mullen,

2008)}. In this research, there degrees of freedom is 190 as compared to the 20 variables.

Further, an improved metric to GFI is the AGFI which adjusts the GFI based upon degrees of freedom, with more saturated models reducing fit {(Tabachnick & Fidell, 2007) as cited in (Hooper, Coughlan, & Mullen, 2008)}. Given that the proposed model meets the AGFI threshold, and GFI is in the range of 0.9 to 0.95, the revised Iteration 2 model fit can be accepted.

5.18 ANSWER TO CENTRAL RESEARCH QUESTION – CRQ

The original EFA identified six factors that enhance cyber security in the Indian Power Sector. The subsequent path model analysis and measures of the model fit using Confirmatory Factor Analysis narrowed down the factors to five that are significant. The five factors are summarized in the Figure 5-9 below.

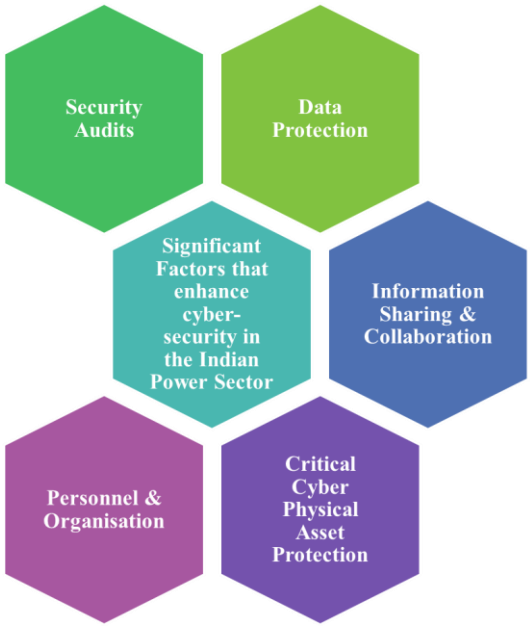

Figure 5-9: Significant Factors that enhance cyber security in the Indian Power Sector

This answers the second part of the Central Research Question.

5.19 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 Power Sector or the research question 1 (RQ 1) was answered using the qualitative research. The Central Research Question which was to identify the factors that enhance cyber security and their significance was answered by the quantitative analysis.

The qualitative analysis established the drivers and need for cyber security in the Indian Power Sector and the need for regulatory intervention. The in-depth interviews helped narrow down the variables to a smaller set of 20 that were relevant to the Indian scenario. These variables were the input for the quantitative analysis to answer the CRQ. The reliability and validity was established. The exploratory factor analysis helped identify the initial set of six factors - Data Protection, Information Sharing & Collaboration, Critical Cyber-Physical assets protection, Personnel & Organization, Risk Assessments and Security Audits that enhance cyber security in the Indian Power Sector. The subsequent confirmatory factor analysis established Data Protection, Information Sharing & Collaboration, Critical Cyber-Physical assets protection, Personnel & Organization, Risk Assessments as significant factors in the Indian context.

6 CONCLUSION AND RECOMMENDATION

6.1 OVERVIEW

This section reviews the recommendations for enhancing cyber security in the Indian Power Sector. The constituents of the mandate that would enhance the cyber security for the Indian Power Sector – (i) Data Protection, (ii) Information Sharing and Collaboration, (iii) Critical Cyber Asset Protection (iv) Personnel and Organization and (v) Security Audits are discussed. The subsequent section in this chapter highlights the research contribution and opportunities for further research.

6.2 CONCLUSION

The objective of the research was to identify the constituents of the cyber security mandate for the Indian Power Sector. The framework analysis of the in-depth interview with experts in the power sector identified the key challenges in the Indian Power Sector and helped identify the variables that are relevant to the Indian context. The validated variables were the inputs to the 5 point Likert-type scale for data gathering that was administered to the respondents. The quantitative analysis of the data, using exploratory factor analysis narrowed down the six factors that would enhance cyber security in the Indian Power Sector. Confirmatory Factor Analysis identified the significant factors that

would should be the constituents of the cyber security mandate for the Indian Power Sector.

There has been a significant investment in building ICT infrastructure in the Indian Power Sector triggered by the Government of India's R-APDRP program. The R-APDRP has ushered in an automation across number of areas – base-lining of assets, building the IT infrastructure for energy auditing, implementation of SCADA / DMS, implementation of IT systems for billing, payment and for improved customer services. The ICT and automation initiatives under the aegis of the R-APDRP has been successful in reducing the AT&C losses in the Indian Power Sector. The increased automation also brings with it an increased threat surface and a susceptibility to cyber vulnerabilities. There awareness of cyber threat is low across at both the board level and within the rank and file in the power sector. This would suggest that the adoption of security management systems within the power sector is not uniform and is very thinly spread, with only a handful of companies have implemented a robust security management framework. Cyber security is often seen as an extension of the IT function and subsumed with the IT teams of the organization at best or deemed as a responsibility that will be delivered by the vendor or SI partner. Designating a senior executive, mandated to assure cyber security combined with a focussed campaign on increasing cyber security awareness can go a long way in addressing this issue.

The diversity of the Indian Power Sector and the financial constraints plaguing the sector, an intervention in the form of a principle based security mandate by the CERC is regarded as the preferred vehicle to enhance cyber security in the power sector.

Data security in the Indian power sector is largely seen as restricted to protection of customer's financial data. This needs to expand to protection of consumption records and mandatory disclosure of data loss and implementing punitive measures for data loss.

Cyber-physical systems are a key component of the infrastructure in power plants. Protection requirements of cyber-physical or control systems in the Operations Technology (OT) domain demand a differentiated approach from data protection in the traditional domain. The identification of critical cyber-physical assets and security certifications of the products that go into the power sector utilities would contribute to enhanced security.

Security Audits both internal within the organisation and third party audits would be the barometer to measure the implementation and the effectiveness of the security controls put in place by the organisations. The audit function essentially is the management eye into the security posture.

A cost effective way to enhance the cyber security posture is to facilitate information sharing and collaboration in the sector. This would ensure diffusion of best practices, increase in security awareness and sharing of threat intelligence.

6.3 RECOMMENDATIONS

In today's networked world, critical infrastructure protection is national priority. The energy sector bears the brunt of cyber threats globally with nearly half the cyber-attacks on critical infrastructure targeting the energy sector. India's power sector is beleaguered with a number of issues but would need to make cyber security a priority and would need to respond swiftly to protects its wellbeing and ensure continued economic growth and prosperity. The recommendations coming out of the research are articulated below:

(i) Mandatory Cyber Security Guidelines for the Power Sector

The CERC should formulate the cyber security guidelines for the Indian Power Sector. The mandatory guidelines should be principle focussed, i.e. focus on broad based standards instead of specific rules. The

guideline should be outcome based and enforce senior management responsibility and accountability. The factors that enhance cyber security in the power sector and that should be included in the guidelines are covered in the subsequent recommendations.

(ii) Personnel & Organisation

A designated senior executive should be made accountable for cyber security of the organisation. Organisations should be tasked with creating a security aware culture and combined with compulsory background screening and whetting of employees.

(iii) Data Protection

The guidelines should detail the identification and protection of customer sensitive data across the entire data lifecycle including data retention requirements. Disclosure of data breach should be made mandatory with suitable financial penalties.

(iv) Critical Cyber-Physical Asset Protection

CERC should articulate the security certifications that are required for critical cyber-physical assets in the power sector. Organisations should identify, maintain a baseline their critical cyber-physical assets. These assets should be subject to period security audits.

(v) Information Sharing & Collaboration (IS&C)

Organisations should be tasked to set up a critical incident response team and define the process to react to a cyber-emergency. CERC should facilitate the setup of a forum for the players in the power sector and promote information sharing and collaboration including disclosure of cyber security incidents.

(vi) Security Audits

Organisations should be mandated to conduct self-assessments for evaluating their cyber security posture apart from periodic third party security audits. CERC should facilitate Industry wide security drills to prepare the organisations to handle a real life cyber –security incident.

Automation and IT proliferation in the power sector is a given, in fact is a dire need in the Indian Power Sector. The government should ensure that while it is promoting the larger adoption of IT, it does not expose an Achilles heel. Formulating and mandating the cyber security guidelines for the power sector will go a long way in addressing this requirement and enhance India's security posture.

6.4 RESEARCH CONTRIBUTION AND THEORETICAL CONSTRUCT

The research identified the constituents of the cyber security mandate in the Indian Power Sector. The research helped narrow down to five significant factors that would contribute to enhancing the security posture in the Indian Power Sector. The five factors are

i.) Data Protection
ii.) Personnel and Organisation
iii.) Critical Cyber-physical asset protection
iv.) Information sharing and collaboration
v.) Security Audits

Laudon and Trevor proposed 4 layer cyber security model for the e-commerce sector includes Data Protection, Technology, Organisation Policies and Procedures with Laws & Industry standards forming the outermost concentric circle.

Each of the areas of recommended factors that enhance cyber security in the power sector i.e. Data Protection, Personnel and Organisation, Information

sharing and collaboration and security audits, cap map to the four layer model recommended by Laudon and Traver for e-commerce security.

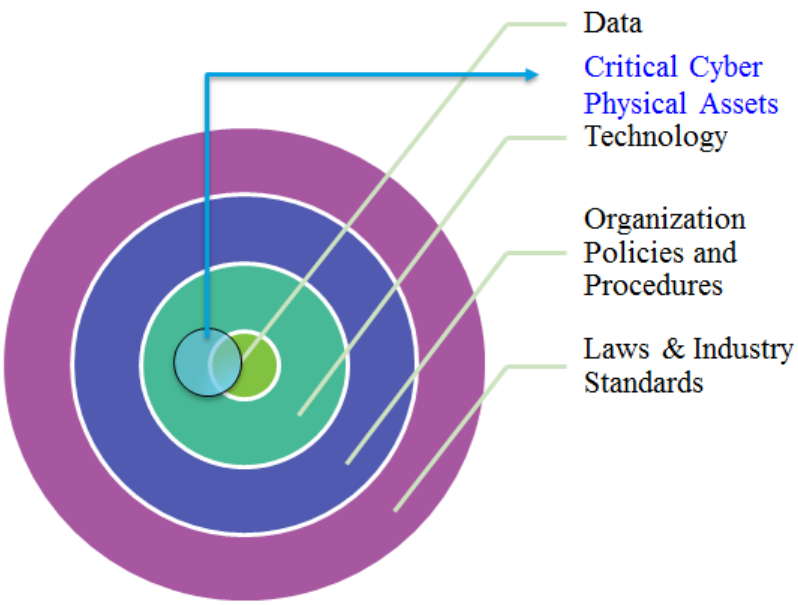

Figure 6-1: 4 layer cyber security model extended for the Power sector

However, the power sector also brings with it the nuance of protection of cyber-physical assets which does not play a role in the e-commerce world. In the power sector co-embedded with the data to be protected we would need to include critical cyber-physical assets The contribution to theory from this research is the extension of the Laudon and Trevor's 4 layer e-commerce security model by including cyber-physical assets when it comes to cyber-security for the power sector. While we have tested the model for the power sector, this revised model that includes cyber-physical asset protection can potentially be expanded to all asset heavy industries.

6.5 LIMITATIONS OF THE STUDY

The research study was focussed on identifying the constituents of the cyber security mandate for the power sector. Five factors were identified that would

enhance the cyber security posture of the Indian Power Sector and tested for its significance. The study however has some limitations:

i.) The extent of the study was limited to India, thus while the model espoused in this study of statistical analysis to identify factors and establishing their significance has universal appeal, this model cannot be extrapolated to other geographies or nations. This is because the choice of the variables, the sample size and extent were all limited to India.

ii.) Cyber security in the power sector is still nascent in India, with very little published literature. The results from the in-depth interviews of the respondents or the survey would be built on their perceptions and these could change with their increased exposure and experience in the sector. This may affect the outcome

iii.) There is minimal published literature on the cyber security policy and guidelines of the Government of India or the roles played by various departments within the government. The research has used publically available data for understanding and interpreting the cyber security polices of the Government of India.

iv.) This research used Principal component analysis for Exploratory Factor Analysis and Orthogonal rotation for extraction of factors. A different choice of statistical techniques may impact the original set of factors.

v.) There is no unanimity on the choice of threshold metrics to define model fit for the Confirmatory Factor Analysis. Different choice of thresholds and metrics could impact the choice of factors.

6.6 FUTURE SCOPE OF THE STUDY

There are a number of opportunities for research scholars to extend this study. The future scope of the study is as follows:

i.) The study examined the power sector as whole, there is an opportunity for researchers to study and recommend the cyber security factors for each of the players in the power generation value chain – Generation, Transmission and Distribution and identify nuances specific to each segment.

ii.) Scholars can undertake a longitudinal research to compare and contrast the security posture of an organisation in the power sector before and after implementation of the security guidelines identified in this study.

iii.) Scholars can study the effectiveness of the Indian IT Act 2000 and other existing cyber law provisions to understand the suitability of the existing legal framework or suggest enhancements to enforce the mandatory compliance regime suggested in this study.

6.7 CONCLUDING REMARKS

The research study identified the five factors that enhance cyber security in the Indian Power Sector. This section called out the recommendations and the contribution to the literature that was the outcome of this research. The study resulted in extending Laudon and Trevor's 4 layer security model by adding a fifth element of critical cyber-physical asset protection in the power sector. The chapter also recognised the limitations of the current research and provides direction for scholars to extend the study in the future.

7 APPENDIX A: INTERVIEW PROTOCOL

i) How has the role of IT evolved in your organization or the power sector? Is there a trend that you have noticed?

ii) With IT and automation, what are the cyber security issues or challenges that you see in the Indian power sector?

iii) How have you tried to address this?

iv) Are security accreditations or certifications a common approach to address security?

v) Do you have or know examples of organizations with a nominated Executive leader responsible for security

vi) Globally we are seeing an increase in regulatory intervention to address cyber security, what has been your experience in Indian power sector.

vii) Regulations can be of two types – Prescriptive, PCI for example is a prescriptive regulation or we could have regulation that is more Principal based or normative. What would be the right approach in India? Why?

viii) What should be the focus areas that needs to be addressed in the regulations?

8 APPENDIX B: QUESTIONNAIRE

8.1 INTRODUCTION

Thank you agreeing to participate in the survey on the cyber security for the power sector in India. This survey is part of a doctoral research in cyber security for the power sector in India. This research is being done in the University of Petroleum and Energy Studies, Dehradun. No individual results or personal information will be shared with any third party. Data will be used only in aggregated form for analysis and interpretation. This form has 22 questions and the entire survey should not take more than 15 minutes of your time. Thank you once again.

Researchers: V. Anand Kumar, Dr. Krishan K. Pandey, Dr. Devendra K. Punia

8.2 INFORMATION SHARING AND COLLABORATION

Section Brief: This section is focussed on evaluation the need to put in place a domain specific information sharing and collaboration process for cyber security in the power sector. It seeks to evaluate the need to make security breach mandatory. (Mark only one oval)

1. There is a need to set up a power industry specific collaboration forums to share security knowledge, incidents and best practices.

◯	Strongly Disagree
◯	Disagree
◯	Neither Agree nor Disagree
◯	Agree
◯	Strongly Agree

2. Disclosure of breaches and security incidents to a nodal agency should be made mandatory for companies in the power sector
   (Help Text: The nodal agency in this case could be the CERT-In or industry specific body under CERC set up to promote information sharing and collaboration)

3. It is important for the nodal agency to main a current directory of industry wide cyber security emergency response contacts

◯	Strongly Disagree
◯	Disagree
◯	Neither Agree nor Disagree
◯	Agree
◯	Strongly Agree

8.3 SECURITY AUDITS, ASSESSMENTS & CERTIFICATIONS

Section Brief: Audits and Self-Assessments seek to validate the compliance to pre-defined security controls. (Mark only one oval)

4. Organisations should undertake quarterly security self-assessments.
   (Help Text: Self assessments would involve organizations evaluating their security posture against a specific set of controls)

◯	Strongly Disagree
◯	Disagree
◯	Neither Agree nor Disagree
◯	Agree
◯	Strongly Agree

5. Annual third party security assessments should be made mandatory in the power sector

◯	Strongly Disagree
◯	Disagree
◯	Neither Agree nor Disagree
◯	Agree
◯	Strongly Agree

6. Periodic Industry wide cyber security drills should be conducted in the power sector.

   (Help Text: Industry wide cyber drills would help identify Inter-dependency between the organisations)

◯	Strongly Disagree
◯	Disagree
◯	Neither Agree nor Disagree
◯	Agree
◯	Strongly Agree

8.4 CRITICAL CYBER-PHYSICAL ASSETS

(Section Brief: Critical Cyber-Physical Assets are essential to the operations of the plants – for e.g. Control Systems, SCADA platforms, and sub-station automation systems) (Mark only one oval)

7. Organisation should identify and maintain a current database of critical cyber-physical assets.

◯	Strongly Disagree
◯	Disagree
◯	Neither Agree nor Disagree
◯	Agree

◯	Strongly Agree

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

   (Help Text: Product security certifications would involve testing the product against security compliance standards)

◯	Strongly Disagree
◯	Disagree
◯	Neither Agree nor Disagree
◯	Agree
◯	Strongly Agree

9. There is a need to review and validate configuration of critical cyber-physical assets

   (Help Text: An example of configuration audit will be to check for default passwords, logging and monitoring configurations changes for critical assets)

◯	Strongly Disagree
◯	Disagree
◯	Neither Agree nor Disagree
◯	Agree
◯	Strongly Agree

8.5 PERSONNEL & ORGANISATION

(Section Brief: Critical Cyber-Physical Assets are essential to the operations of the plants – for e.g. Control Systems, SCADA platforms, and sub-station automation systems) (Mark only one oval)

10. Organisation should identify and nominate a senior executive responsible for security to report to the Board.

    (Help Text: For e.g. the Reserve Bank of India mandates that a senior executive should be nominated as the person responsible for information security in the bank)

◯	Strongly Disagree
◯	Disagree
◯	Neither Agree nor Disagree
◯	Agree
◯	Strongly Agree

11. Cyber Security education and training should be mandated for all employees in the power sector.

◯	Strongly Disagree
◯	Disagree
◯	Neither Agree nor Disagree
◯	Agree
◯	Strongly Agree

12. 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

8.6 PRIVACY AND SENSITIVE DATA PROTECTION

(Section Brief: The operators in the power sector are the custodians of customer sensitive information. This section deals with privacy and data protection requirements.) (Mark only one oval)

13. Companies should put in place security controls to ensure protection of customer sensitive information.

◯	Strongly Disagree
◯	Disagree
◯	Neither Agree nor Disagree
◯	Agree
◯	Strongly Agree

14. Electricity consumption data records of customers should be classified and protected sensitive data.

    (Help Text: Like "Call Data Records" in the telecom sector, power consumption data can be potentially misused in the era of smart meters)

◯	Strongly Disagree
◯	Disagree
◯	Neither Agree nor Disagree
◯	Agree
◯	Strongly Agree

15. The policy should define data retention and data purging requirements.

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

16. There should financial penalties enforced on operators for loss of customer sensitive information.

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

17. Breach disclosures of customer sensitive information should be enforced.

    (Help Text: Companies should be mandated to put in place a process to intimate end users and publically disclose loss of customer sensitive information)

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

8.7 RISK ASSESSMENTS

(Section Brief: Security controls should be aligned to risk. The section deals with the process and need to conduct risk assessments.) (Mark only one oval)

18. Power sector organisation should conduct a baseline risk assessment and arrive at a risk score.

◯	Strongly Disagree
◯	Disagree
◯	Neither Agree nor Disagree
◯	Agree
◯	Strongly Agree

19. Risk assessments should be reviewed periodically

◯	Strongly Disagree
◯	Disagree
◯	Neither Agree nor Disagree
◯	Agree
◯	Strongly Agree

20. Security controls aligned to the risk must be reviewed periodically for effectiveness and performance threshold established.

◯	Strongly Disagree
◯	Disagree
◯	Neither Agree nor Disagree
◯	Agree
◯	Strongly Agree

8.8 OTHERS

21. In your opinion, what other aspects of cyber security or governance should be included in the national cyber security policy for the power sector in India.
    (Free Text answer)

22. How would you describe yourself? Pl chose the closest that applies to you. (Mark only one oval)

⬭	Policy maker / Government Sector / Academician
⬭	Power sector professional
⬭	System Integrator or Security professional / Security Auditor

9 APPENDIX C: WORKING DEFINITION OF VARIABLES

Sl. No	Variable	Working Definition
1	ISnC	Power sector specific Information sharing and collaboration (ISAC) forums
2	Mandatory Disclosure	Breach disclosures to be made mandatory
3	Computer Emergency Response Team	Industry wide Computer Emergency Response owner
4	Self-Assessments	Self-assessments are check list based assessments against defined security controls
5	Security Drills	Security drills would simulate a cyber-attack to evaluate response and preparedness.
6	Industry wide Drills	Security drills that simulate a simultaneous cyber-attack on number of organisations and evaluate response and preparedness
7	Critical Cyber-physical assets / systems	Control systems and components of the Operations Technology domain like SCADA, Sub-station automation and control systems.
8	Product Security certifications	Third party certifications to ensure security posture of the product an example will be the Common Criteria certifications.
9	Configurations Review	Security review of components of Critical Cyber-physical systems

Sl. No	Variable	Working Definition
10	Senior Executive responsible for Security	A senior executive like a "CISO" or Chief Information Security Officer who is the nominated individual responsible for cyber security.
11	Security Education & Awareness	Security training and education of the staff
12	Screening & Background Verification	Background verification and security clearance for employees working in or having access to critical cyber systems.
13	Sensitive Data Protection	Protection of Personally Identifiable information and sensitive data like Credit card numbers or combination of one or more data that will personally identify a consumer.
14	Consumption Data Records	Detailed electricity consumption records that are available as part of smart metering roll outs
15	Data Retention Guidelines	Data lifecycle requirements that identify the data types and duration for retention, storage and purging.
16	Financial Penalties	Fines and penalties for loss of customer sensitive data
17	Mandatory Breach Disclosure	Disclosure of data loss to impacted individuals and public disclosure of data loss
18	Baseline Risk Assessments	Risk Assessments to identify risks, risk treatments and residual risks
19	Periodic Risk Review	Review of the risks periodically to validate any change in risk posture
20	Security effectiveness and performance thresholds	Security metrics to measure effectiveness of controls established and performance and trending of security data.

10 BIBLIOGRAPHY

Government of India, Ministry of Telecommunications & IT, Department of Telecommunications. (2012, June 13). National Telecom Policy - 2012. New Delhi, New Delhi, India.

Alpcan, T. (2010). *GameSec 2010.* Retrieved Aug 15, 2013, from Gamesec-conf.org: http://www.gamesec-conf.org/2010/GameSec2010_Introduction-new.pdf

Anderson, R., & Fuloria, S. (2011, September 15). *Smart meter security: a surver*. Retrieved June 16, 2012, from Computer Laboratory Faculty of Computer Science and Technology: http://www.cl.cam.ac.uk/~rja14/Papers/JSAC-draft.pdf

Anderson, R., & Fuloria, S. (2011, September 15). *Smart meter security: A survey*. Retrieved June 16, 2012, from Computer Laboratory Faculty of Computer Science and Technology: http://www.cl.cam.ac.uk/~rja14/Papers/JSAC-draft.pdf

Anderson, R., Moore, T., Nagaraja, S., & Ozment, A. (2007). Incentives and information security. In T. R. Noam Nisan (Ed.), *Algorithmic Game Theory* (pp. 633 - 649). NY: Cambridge University Press.

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

Bajaj, H., & Sharma, D. (2006, Dec 12 - 15). Power Sector Reforms in India. *Power Electronics, Drives and Energy Systems, 2006. PEDES '06 International Conference on*, (pp. 1-5).

Baker Institute Policy Report. (2012). *Cyber Security Issues and Policy Options for the U.S. Energy Industry*. James A. Baker III Institute of Public Policy of Rice University, The.

Bangalore Electricity Supply Company. (2015, Oct 3). *Creation of Information Technology and Smart Grid Cadre.* Retrieved Nov 1, 2015, from BESCOM.ORG: http://bescom.org/wp-content/uploads/2015/10/Creation-of-Information-Technology-and-Smart-Grid-Cadre.pdf

Barnes, E. (2010, Nov 26). *Mystery Surrounds Cyber Missile That Crippled Iran's Nuclear Weapons Ambitions*. (F. News, Producer) Retrieved Oct 2, 2012, from FoxNews.com: http://www.foxnews.com/scitech/2010/11/26/secret-agent-crippled-irans-nuclear-ambitions/print

Black, J., Hopper, M., & Band, C. (2007, May). Making a success of Principles-based regulation. *Law and Financial Markets Review*, 191 - 206.

Bronk, C., & Tikk-Ringas, E. (2013, Feb 1). *Hack or Attack? Shamoon and the evolution of cyber conflict.* Retrieved Apr 14, 2014, from James A. Baker III Institute of Public Policy Rice University: http://bakerinstitute.tendenciapp.com/media/files/Research/dd3345ce/ITP-pub-WorkingPaper-ShamoonCyberConflict-020113.pdf

Brown, A. (2002, December). SCADA vs the hackers, can freebie and a can of Pringles bring down the U.S. power grid? *Mechanical engineering, 124*(12).

Brown, C. H., Klopp, M. P., Palmer, C. C., & Wolf, D. G. (2014). *The Science of Security.* AFCEA International Cyber Committee. Retrieved from http://www.afcea.org/mission/intel/documents/ScienceofSecurityFinal.pdf

Brown, G. D. (2011, Oct). *National Defense University Press*. Retrieved July 2012, from Joint Forces Quarterly: http://www.ndu.edu/press/why-iran-didnt-admit-stuxnet.html

Bryman , A., & Bell , E. (2011). *Business Research Methods 3/e*. New Delhi: Oxford University Press.

Bryman , A., & Bell, E. (2011). *Business Research Methods 3/e*. New Delhi: Oxford University Press.

Bryman, A., & Bell, E. (2011). *Business Research Methods 3/e*. New Delhi: Oxford University Press.

Bryman, A., & Bell, E. (2011). *Business Research Methods 3/e*. New Delhi: Oxford University Press.

Bryman, A., & Bell, E. (2011). *Business Research Methods 3/e*. New Delhi: Oxford University Press.

Bryman, A., & Bell, E. (2011). *Business Research Methods 3/e*. New Delhi: Oxford University Press.

Bryman, A., & Bell, E. (2011). *Business Research Methods 3/e*. New Delhi: Oxford University Press.

Bryman, A., & Bell, E. (2011). *Business Research Methods 3/e*. New Delhi: Oxford University Press.

Bryman, A., & Bell, E. (2011). *Business Research Methods 3/e*. New Delhi: Oxford University Press.

Bryman, A., & Bell, E. (2011). *Business Research Methods 3/e*. New Delhi: Oxford University Press.

Bryman, A., & Bell, E. (2011). *Business Research Methods 3/e*. New Delhi: Oxford University Press.

Bryman, A., & Bell, E. (2011). *Business Research Methods 3/e*. New Delhi: Oxford University Press.

Bryman, A., & Bell, E. (2011). *Business Research Methods, 3/e.* New Delhi: Oxford University Press.

Bryman, A., & Bell, E. (2011). *Business Research Methods, 3/e.* New Delhi: Oxford University Press.

Bryman, A., & Bell, E. (2011). *Business Research Methods, 3e.* New Delhi: Oxford University Press.

Bulmer, M. (1984). *Facts, Concepts, Theories and Problems.* London: MacMillan.

Byres, E. (2013, Aug). The Air Gap: SCADA's Enduring Security Myth. *Communications of the ACM, 56*(8), 29 - 31.

c4 Security. (n.d.). *The Dark Side of the Smart Grid - Smart Meter (in)Security.* Retrieved July 15, 2012, from c4-security | Resources : http://www.c4-security.com/The%20Dark%20Side%20of%20the%20Smart%20Grid%20-%20Smart%20Meters%20%28in%29Security.pdf

Cabinet Office, United Kingdom. (2010, Mar). *Strategic Framework and Policy Statement on improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards.* Retrieved July 19, 2014, from Centre for Protection of National Infrastructure: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62504/strategic-framework.pdf

Cattell, R. (1978). *The Scientific Use of Factor Analysis.* New York : Plenum.

Central Electric Authority. (2012, Dec). *Central Electric Authority - Monthly Exec Reports.* Retrieved Feb 11, 2013, from Central Electric Authority: http://www.cea.nic.in/reports/monthly/executive_rep/dec12/1-2.pdf

Central Electricity Authority. (2015, Nov). *All India Installed Capacity of Power stations*. Retrieved Dec 11, 2015, from Central Electricty Authority:

http://www.cea.nic.in/reports/monthly/installedcapacity/2015/installed_capacity-11.pdf

Cert-In. (2011). *Cert-In Annual Report 2010-11*.

Clemente, J. (2009, June). The Security Vulnerabilities of Smart Grids. *Journal of Energy Security*.

Cooper, H. (1988). Organizing knowledge syntheses: A taxonomy of literature reviews. *Springer*, 104 - 126. doi:http://dx.doi.org/10.1007/BF03177550

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

Date, J. (2010, June 27). *thisweek with George Stephanopoulos.* Retrieved May 1, 2012, from ABCNews.com: http://abcnews.go.com/ThisWeek/cia-director-panetta-exclusive-intelligence-bin-laden-location/story?id=11027374&page=2

Deng, Y., & Shukla, S. (2012). Vulnerabilities and Countermeasures - A Survey on the Cyber Security Issues in the Transmission Subsystem of a Smart Grid. *Journal of Cyber Security and Mobility, I*, 251 - 276.

Department of Business Innovation & Skills. (2013). *UK Cyber Security Standards.* Department of Business Innovation & Skills. Retrieved May 1, 2014

Department of Commerce, US Government Publishing Office. (1998, Aug 5). *Federal Register Volume 63, Issue 150* . Retrieved from US Government Publishing Office: http://www.gpo.gov/fdsys/granule/FR-1998-08-05/98-20865

Department of Electronics and Information Technology. (n.d.). *Strategic Approach*. Retrieved July 15, 2015, from Department of Electronics and Information Technology: http://deity.gov.in/content/strategic-approach

Department of Homeland Security. (2003, Feb). *The National Strategy to Secure the Cyberspace.* Retrieved July 19, 2014, from The US-Cert: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

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

ENISA - European Network and Information Security Agency. (2012). *Smart Grid Security.* Brussels: European Network and Information Security Agency (ENISA).

ENISA. (2011). *Protecting Industrial Control Systems: Recommendations for Europe and Member States.* ENISA. Retrieved from https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states/at_download/fullReport

ENISA. (2012). *Smartgrid Security: Recommendation for Europe and Member States.* European Commission, ENISA. ENISA. Retrieved from https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA-smart-grid-security-recommendations/at_download/fullReport

ENISA. (n.d.). *Incident Reporting and Security regulation*. Retrieved Feb 11, 2015, from ENISA: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting

Ernst & Young. (2011 , Dec). *Attacking the Smart Grid Penetration testing techniques for industrial control systems and advanced metering infrastructure.* Retrieved Jan 26, 2013, from Ernst & Young Publication: http://www.ey.com/Publication/vwLUAssets/Attacking_the_smart_grid/$FILE/Attacking-the-smart-grid_AU1058.pdf

Euractiv. (2013, Mar 8). *EU, US go separate ways on cybersecurity*. Retrieved Apr 9, 2013, from Euractiv: http://www.euractiv.com/specialreport-cybersecurity/eu-us-set-different-approach-cyb-news-518252

European Commission . (2013). Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union. *COM(2013) 48 final, 2013/0027 (COD)*. Brussels: European Commission.

Europeon Commission. (2009, Mar 9). *"Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience.* Retrieved April 14, 2012, from European Commission: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

Everitt, S. (1975). Multivariate analysis: The need for data, and other problems. *British Journal of Psychiatry, 2S7-240*, 126.

Falk, R., & Fries, S. (2011). Smart Grid Cyber Security - An Overview of Selected Scenarios and Their Security Implications. *34 Pages 168-175*.

Fundación BBVA. (2014). *Multivariate Statistics' Project*. Retrieved Jan 26, 2015, from Fundación BBVA: http://www.multivariatestatistics.org/

Gartner Inc. (n.d). *Gartner IT Glossary*. Retrieved Oct 1, 2015, from Gartner.com: www.gartner.com/it-glossary/operational-technology-ot

Gaskin , J. (2012). *Confirmatory Factor Analysis*. Retrieved Jan 26, 2015, from Gaskination's StatWiki: http://statwiki.kolobkreations.com/wiki/Confirmatory_Factor_Analysis

Gaskin, J. (2012). *Exploratory Factor Analysis*. Retrieved Jan 26, 2014, from Gaskination's Statwiki: http://statwiki.kolobkreations.com/wiki/Exploratory_Factor_Analysis

Gaskin, J. (2012). *Stattools Package*. Retrieved Feb 11, 2015, from www.kolobkreations.com: http://statwiki.kolobkreations.com

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

Gorsuch, E. (1983). *Factor Analysis 2/e.* Hillsdale, NJ: Eribaum.

Government of India, Central Electricity Authority (CEA). (2013). *Central Electricity Authority*. Retrieved September 22, 2013, from Cyber Threats and Security for the Power Sector: www.cea.nic.in

Government of India, Ministry of Communications & IT, Department of Telecommunications (Access Services Wing). (2011, May 31). Amendment to the Unified Access Service License Agreement for security related concerns for expansion of Telecom Services in various zones of the the country. New Delhi, New Delhi, India. Retrieved May 1, 2012, from Department of Telecommunications Website: http://www.dot.gov.in/AS-III/2011/as-iii.pdf

Government of India, Ministry of Communications and IT. (2013, July 02). *National Cyber Security Policy 2013.* Retrieved July 05, 2013, from www.deity.gov.in: http://deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1).pdf

Government of India, Ministry of Communications and IT, Department of Electronics and Information Technology. (2013, July 02). *National Cyber Security Policy 2013.* Retrieved July 05, 2013, from www.deity.gov.in: http://deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1).pdf

Government of India, Ministry of Power. (2008, July 8). *Continuation of Restructured Accelerated Power Development and Reforms Program (R-APDRP) in XII and XIII Plan.* Retrieved Dec 1, 2015, from Apdrp.gov.in: http://www.apdrp.gov.in/OrderSGuidelines/R-APDRP_in_XII_XII_plan.pdf

Government of India, Ministry of Power. (2015, Mar 19). *AT&C losses.* Retrieved July 27, 2015, from Powermin.nic.in: http://powermin.nic.in/upload/loksabhatable/pdf/LS19032015_Eng.pdf

Government of India, Northern Regional Power Committee. (2014, Sept 15). *103rd meeting of the Operation Co-ordination Sub-committee.* Retrieved Dec 25, 2014, from NRPC.GOV.IN: http://www.nrpc.gov.in/Meetings/OCC/OCC103/OCC103_AA1.pdf

Gross, M. J. (2011, April). *Vanity Fair.* Retrieved Aug 2012, from www.vanityfair.com: http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104

Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1995). *Multivariate data analysis 4/e.* Saddle River, NJ: Prentice Hall.

Hair, J., Black, W., Babin , B., & Anderson, R. (2010). *Multivariate data analysis 7/e.* Upper Saddle River: Prentice-Hall, Inc.

Hale, G. (2011, Mar 23). *Industrial Safety and Security Source.* Retrieved Aug 2012, from www.isssource.com: www.isssource.com/more-scada-vulnerabilities-found/

Hansel, M. (2013, Jun 27). *Cyber Security Governance and the Theory of Public Goods*. Retrieved Oct 2, 2014, from E-International Relations: http://www.e-ir.info/2013/06/27/cyber-security-governance-and-the-theory-of-public-goods/

Hart, C. (1998). Doing a literature review: Releasing the social science research imagination. .

Hellstorm, T. (2007). Critical infrastructure and systemic vulnerability: Towards a planning framework. *45*(3; Pages 415-430).

Hespanha, J. P. (2002). Game Theory and Network Security. *Proc. of the GAMBIT Workshop: A DARPA Sponsored Research Summit.* Retrieved from University of California at Santa Barbara: http://www.ece.ucsb.edu/~hespanha/published/HespanhaNetworkSecurityMay31.pdf

Hoffman, D. E. (2004, Feb 27). *WashPost: CIA slipped bugs to Soviets.* Retrieved June 2012, from Industrial Defender: http://industrialdefender.com/general_downloads/incidents/1982.06_trans_siberian_gas_pipeline_explosion.pdf

Hooper, D., Coughlan, J., & Mullen, M. (2008). Structural Equation Modelling: Guidelines for Determining Model Fit. *Electronic Journal of Business Research Methods, 6*(1), 53-60.

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.

Hutcheson, G. S. (1999). *The multivariate social scientist: Introductory statistics using generalized linear models.* Thousand Oaks: Sage Inc. Retrieved from Hutcheson, G., & Sofroniou, N. (1999). The multivariate social scientist: Introductory statistics using generalized linear models. Thousand Oaks, CA: Sage Publications

India Smart Grid Forum. (2012). *Smart Grid Vision & Roadmap for India (benchmarking with other countries) - Final Recommendation from ISGF.*

Indian Computer Emergency Response Team (CERT-In). (2007, Mar 31). *Annual Report (2006).* Retrieved April 2, 2015, from Department of Electronics and Information Technology: http://www.cert-in.org.in/

Indian Computer Emergency Response Team (Cert-In). (2015, Feb 27). *Annual Report (2014).* Retrieved May 1, 2015, from Department of Electronics and Information Technology: http://www.cert-in.org.in/

Indian Power Sector. (n.d.). *History of Indian Power Sector.* Retrieved Jan 11, 2013, from Indian Power Sector: http://indianpowersector.com/home/about/overview/

Indian Power Sector. (n.d). *History of Indian Power Sector*. Retrieved Dec 2, 2015, from Indian Power Sector: http://indianpowersector.com/about/overview/

Information Warfare Monitor and Shadowserver Foundation. (2010, April 6). *Shadows in the Cloud: Investigating Cyber Espionage 2.0.* Retrieved May 1, 2013, from Data Security Council of India: https://www.dsci.in/node/506

Institute for Defense Studies and Analysis. (2012). *India's Cyber Security Challenges.* New Delhi: Institute for Defense Studies and Analysis.

Internet world stats. (2012, June 30). *Internet users in Asia*. Retrieved Mar 15, 2014, from Internetworldstats.com: http://www.internetworldstats.com/stats3.htm

JASON, The Mitre Corporation. (2010). *Science of Cyber-security.* McClean: The Mitre Corporation. Retrieved from http://fas.org/irp/agency/dod/jason/cyber.pdf

Kenny, D. A. (2011, Sept 11). *Respecification of Latent Variable Models.* Retrieved Jan 26, 2015, from David kenny's Homepage: http://davidakenny.net/cm/respec.htm

Kline, P. (1979). *Psychometrics and psychology.* London: Academic Press.

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

Kobayashi, B. (2011, May). *An economic analysis of the private and social costs of the provision of cybersecurity and ohter public security goods.* Retrieved Apr 14, 2014, from Social Science Research Network: ssrn.con/abstract_id=708562

Kothari, C. (2013). *Research Methodology.* New Delhi: New Age International (P) Ltd.

Kothari, C. R. (2013). *Research Methodology 2/e.* New Delhi: New Age International (P) Limited.

Kroger, W. (2008). Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools. *93*(12; Pages 1781-1787).

Kunce, J. T., Cook, W. D., & Miller, D. E. (1975). Random variables and correlational overkill. *Educational and Psychological Measurement, 35*, 529-534.

Lal, R., & Saluja, R. (2012). E Banking: The Indian Scenario. *Asia Pacific Journal of Marketing and Management Review, 1*(4).

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

Langer, R. (2011, Mar 11). *TED Review* - . Retrieved June 2012, from Langner - The last line of Cyber Defense: www.langner.com

Laudon, K., & Trevor, C. (2015). *E-Commerce 2015, 11/E.* New York: Prentice-Hall.

Lawley, D. N., & Maxwell, A. E. (1972). *Factor analysis as a statistical method. London: Butterworth and Co.* London: Butterworth and Co.

Lee, R. M. (2011, May 19). *Stuxnet and the Paradigm Shift in Cyber Warfare*. (Putnam Media) Retrieved July 27, 2013, from Control Global: http://www.controlglobal.com/articles/2011/stuxnet-paradigm-shift-in-cyber-warfare/?show=all

Lewis, J. A. (2010). Soverignty and the Role of Government in Cyberspace. *XVI*(II; Pages 55-65).

Lewis, J. A. (2013, Feb 12). *Raising the Bar for Cybersecurity.* Retrieved May 1, 2013, from Center for Strategic & Internal Studies.

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

Lyytinen, K., & Gaskin, J. (2014, Sept 23). *Exploratory Factor Analysis.* Retrieved Dec 21, 2014, from Statwiki: http://www.kolobkreations.com/Factor%20Analysis.pptx

MacCullum , R., Widaman, K., Zhang, S., & Hong, S. (1999). Sample Size in factor analysis. *Psychological Methods, 4*, 84-89.

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.

Malashenko, E., Villarreal, C., & Erickson, D. J. (2012, Sept 19). *Cybersecurity and the evolving role of State Regulations: How it impacts California Public Utilities commission* . Retrieved Apr 10, 2013, from California Public Utilities Commission: http://www.cpuc.ca.gov/NR/rdonlyres/D77BA276-E88A-4C82-AFD2-FC3D3C76A9FC/0/TheEvolvingRoleofStateRegulationinCybersecurity9252012FINAL.pdf

Malhotra, N., & Dash, S. (2011). *Marketing Research - An applied orientation 6/e.* New Delhi: Pearson Publishing.

McCabe, A. (2014, November 12). *Cybersecurity & Public Utility Commission.* Retrieved Feb 11, 2015, from https://tcipg.org/sites/default/files/slides/iw2014_mccabe_ann.pdf

McGowan, M. L. (2013, May 22). *15 Years After Presidential Decision Directive (PDD) 63*. Retrieved July 27, 2014, from www.boozallen.com: http://www.boozallen.com/media-center/company-news/2013/05/15-years-after-pdd63-blog-post

McKinsey & Co. (2010). *Powering India: The road to 2017.* McKinsey & Co.

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

Miles, J., & Shevlin, M. (1998). Effects of sample size, model specification and factor loadings on the GFI in confirmatory factor analysis. *Personality and Individual Differences, 25*, 85-90.

Mimoso, M. S. (2008, January 15). *Bruce Schneier Reflects on a Decade of Security Trends.* Retrieved May 1, 2012, from Bruce Schneier: http://www.schneier.com/news-049.html

Minichiello, V., Aroni, R., Timewell, E., & Alexander, L. (1990). *In-depth interviewing: Researching people.* Melbourne: Longman Chesire .

Ministry of Finance, Government of India. (2013, Feb). *Plan Outlay - Expenditure Budget Vol1 2012-13.* Retrieved Apr 8, 2013, from India Budget: http://indiabudget.nic.in/ub2012-13/eb/po.pdf

Ministry of Power, Government of India. (2013). *Measures to reduce AT&C Losses.* New Delhi: Press Information Bureau.

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *3, Pages 1 0 3 – 1 1 7*(3-4).

NASSCOM. (n.d.). *Indian IT-BPO Industry*. Retrieved Mar 15, 2014, from NASSCOM: http://www.nasscom.in/indian-itbpo-industry

National Critical Information Infrastructure Protection Centre, NTRO. (2013, June). *Guidelines for National Critical Information Infrastructure Protection.* Retrieved Mar 15, 2014, from www.ficciweb.info: http://www.ficciweb.info/conf-cell/Guidelines.pdf

National Technical Research Organisation. (2013). *Guidelines for Protection of National Critical Information Infrastructure.* New Delhi: National Critical Information Infrastructure Protection Centre.

N-Dimension Solutions Inc. (2015). *Attack Surface*. (N-Dimensions Solutions Inc) Retrieved Oct 24, 2015, from N-Dimension Solutions: http://www.n-dimension.com/critical-infrastructure-threat/attack-surface/

Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). Scada security in the light of Cyber-Warfare. *31*(4; Pages 418-436).

NIST. (2010). *NIST Smart Grid Framework.* Washington: NIST.

North Amercian Electricity Reliabiity Corporation . (n.d.). *CIP Compliance*. Retrieved Feb 11, 2015, from NERC North Amercian Electricity Reliability Corporation: http://www.nerc.com/pa/CI/Comp/Pages/default.aspx

North America Electric Reliability Corporation. (n.d.). *CIP V5 Transition Program*. Retrieved Feb 11, 2015, from NERC North America Electric Reliability Corporation: http://www.nerc.com/pa/CI/Pages/Transition-Program.aspx

Nye, J. S. (2010). *Cyber Power.* Cambridge: Harvard Kennedy School,Belfer Center for Science and International Affairs. Retrieved May 1, 2015

OECD. (2014). *OECD Economic Surveys: India 2014.* OECD Publishing.

Office of Cyber Security and Information Assurance in the Cabinet Office. (2011). *The UK Cyber Security Strategy Protecting and promoting the UK in a digital world.* London: Cabinet Office. Retrieved Mar 22, 2013

Paganini, P. (2013, Oct 27). *Subcontractors are for hackers the weakest link in security chain*. Retrieved Jan 24, 2014, from Security Affairs: http://securityaffairs.co/wordpress/19121/cyber-crime/hacking-subcontractors.html

Patel, S. (2014, 3 26). Cybersecurity Trends Show Overwhelming Energy Sector Vulnerabilties. *Power*. Retrieved from http://www.powermag.com/cybersecurity-trends-show-overwhelming-energy-sector-vulnerabilities/

Patil, S. (2014, June 17). *India's vulnerable SCADA systems*. Retrieved Nov 2, 2014, from Gateway House: http://www.gatewayhouse.in/indias-vulnerable-scada-systems/

Paul, S., Das Gupta, S., Islam, K. A., Saha, K., & Majumder, S. (2012). Challenges of securing the smart grid and their probably security solutions. Singapore: IPCBEE vol 44.

Pearson, I. L. (2011). Smart grid cyber security for Europe. *39*(9; Pages 5211-5218).

Pennyslavania Public Utility Commission. (2013). *Public Utility Commission Cyber security Overview*. Retrieved Feb 11, 2015, from NARUC Meetings: http://www.narucmeetings.org/Presentations/Cyber%20Briefing%202013.pdf

Pollet, J. (2010, July 28). *Black Hat USA Electricity For Free ? The Dirty Underbelly of SCADA and Smart Meters.* Retrieved June 19, 2012, from Cupfighter: http://www.cupfighter.net/index.php/2010/07/blackhatusa-electricity-for-free/

Press Information Bureau. (n.d.). *Indian telecom network now world's 2nd largest*. Retrieved Mar 15, 2014, from Governance Knowledge Centre: http://indiagovernance.gov.in/news.php?id=309

Press Trust of India. (2014, Nov 30). *Cybercriminals target telecom firms in India, other nations with Regin*. Retrieved Nov 30, 2014, from Economic Times: http://articles.economictimes.indiatimes.com/2014-11-30/news/56582820_1_regin-security-solutions-provider-symantec-networks

Press Trust of India. (2015, Aug 7). *Cyber attacks on India mostly from Pakistan, China: Government*. Retrieved Aug 8, 2015, from Economic Times: http://telecom.economictimes.indiatimes.com/news/policy/cyber-attacks-on-india-mostly-from-pakistan-china-government/48393219

Randolph, J. J. (2009). A Guide to Writing the Dissertation Literature Review. *Practice Assessment, Research & Evaluation, 14*(13). Retrieved July 27, 2013, from http://lincs.etsmtl.ca/uploads/media/v14n13.pdf

Renewable Energy Technology. (2013, Jan 28). *Swiss technology for large scale Indian smart metering project* . (Cavandish Inc) Retrieved Mar 15, 2014, from Renewable Energy Technolgy: http://www.renewable-energy-technology.net/grid-energy-storage-news/swiss-technology-large-scale-indian-smart-metering-project

Reserve Bank Of India. (2011, Jan 14). *Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds.* Retrieved Aug 15, 2012, from Reserve Bank of India: http://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WREB210111.pdf

Reserve Bank of India. (2001, June 14). *Internet Banking in India - Guidelines.* Retrieved August 15, 2012, from Reserve Bank of India: rbidocs.rbi.org.in/rdocs/notification/PDFs/21569.pdf

Ritchie, J., & Spencer, L. (1994). Qualitative Data Analysis for Applied Policy Research. In A. a. Bryman, *Analyzing Qualitative Data* (pp. 173 - 194). Taylor and Francis Inc.

Rosenzweig, P. (2011). Cybersecurity and Public Goods The Public/Private "Partnership". *Emerging Threats in National Security and Law*, 1- 36. Retrieved from www.hoover.org: http://www.hoover.org/sites/default/files/research/docs/emergingthreats_rosenzweig.pdf

Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., & Wu, Q. (2010). A Survey of Game Theory as Applied to Network Security. *The 43rd Hawaii International Conference on System Sciences.* Retrieved from http://gtcs.cs.memphis.edu/pubs/hicss43.pdf

Ryu, D. H., Kim, H., & Um, K. (2009). Reducing security vulnerabilities for critical infrastructure. *22*(6; Pages 1020-1024).

Sarkar, M. (2014, Dec 16). *Aggregate Technical & Commercial loss Determination Challenges and its Solution in Indian Scenario.* Retrieved from Utility Analytics Institute: http://www.energybiz.com/article/14/12/aggregate-technical-commercial-loss-determination-challenges-and-its-solution-indian-scenario

Schierholz, R., & Wijs, B. d. (n.d.). *Cyber security in the power and water industries How end users and vendors are or should be facing it.* Retrieved Apr 9, 2013, from ABB: http://www05.abb.com/global/scot/scot296.nsf/veritydisplay/c058a88e143427f3c12578e00053f5a0/$file/3bus095405_l_a_en_cyber_security

_for_the_power_and_water_industrieshow_end_users_and_vendors_are_or_should_be_facing_i.pdf

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.

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.

Sellitz, C. (1962). *Research Methods in Social Sciences.* New York : Holt, Rinehart and Winston.

Sharma, S., Mukherjee, S., Kumar, A., & Dillon, W. (2005). A simulation study to investigate the use of cutoff values for assessing model fit in covariance structure models. *Journal of Business Research, 58*(1), 935-43.

Shiva, S., Roy, S., & Dasgupta, D. (2010). Game Theory for Cyber Security. *Sixth Cyber Security and Information Intelligence Research Workshop.* Oak Ridge.

Smart Grid Interoperability Panel. (2010, Sept). *Introduction to NISTIR 7628 Guidelines to Smart grid cyber Security.* Retrieved May 1, 2013, from Smartgrid.gov: https://www.smartgrid.gov/files/nistir_7628_.pdf

Smart grid Interoperability Panel. (2014, Feb). *NISTIR 7628 User's guide.* Retrieved May 1, 2014, from Smart Grid Interoperability Panel SGIP: http://members.sgip.org/apps/group_public/download.php/3456/NISTIR%207628%20Users%20Guide%20FINAL-2014-02-27c.pdf

Statistics Solution. (2013). *Confirmatory Factor Analysis*. Retrieved Jan 26, 2015, from Statistics Solution: http://www.statisticssolutions.com/academic-solutions/resources/directory-of-statistical-analyses/confirmatory-factor-analysis/

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

Stokes, D. E. (1997). Pasteur's Quadrant. *Brookings Institute*.

Strauss, A., & Corbin, J. (1998). *Basics of Qualitative Research: Techniques and Procedures for developing Grounded Theory* . Thousand Oaks, CA: Sage.

Symantec Corporation. (2011, Aug 18). *Regulatory Compliance Drives Security Adoption in Indian Financial Sector – Symantec Report* . Retrieved Oct 2, 2012, from About Symantec: Press Release : http://www.symantec.com/content/en/in/enterprise/collateral/other_resources/MediaPresentation_SymantecSecurityCheck_Indian%20FinancialServices_SurveyFindings_August18.pdf

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

Tabachnick, B., & Fidell, L. (2007). *Using Multivariate Statistics 5/e.* New York: Allyn and Bacon.

The Hindu Bureau. (2015, Dec 11). Power bonds attractive despite non-SLR tag. *The Hindu Businessline*, p. 1. Retrieved Dec 12, 2015, from http://www.thehindubusinessline.com/todays-paper/power-bonds-attractive-despite-nonslr-tag/article7978028.ece

The White House. (2013, Feb 12). *Executive Orders*. Retrieved Mar 15, 2014, from whitehouse.gov: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

The White House. (2013, Feb 12). *Statements and Releases*. Retrieved Mar 15, 2014, from whitehouse.gov: http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

Tikk, E., Kaska, K., & Vihul, L. (2010). *International Cyber Incidents: Legal Consideration.* Retrieved July 12, 2012, from NATO Cooperative Cyber Defence Centre of Excellence Talinn Estonia: www.ccdcoe.org

TJX Securities Exchange Commission Filing. (n.d.). Form 10K of the annual report filings. *http://www.sec.gov/Archives/edgar/data/109198/000095013507001906/b64407tje10vk.htm*.

Tritschler, M., & Mackay, W. (2011). *UK Smart grid cyber security.* London: Energy Networks Association. Retrieved from http://www.energynetworks.org/modx/assets/files/news/publications/UK%20Smart%20Grid%20Cyber%20Security%20Report.pdf

U.S. Department of Energy. (2012, May). *Electricity Subsector Cybersecurity Risk Management Process.* Retrieved Apr 9, 2013, from Department of Energy: http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf

UK Government. (2010). *A Strong Britain in the Age of Uncertainity: The National Security Strategy.* London: Controller of Her Majesty's Stationery Office.

Urengoy Pomary Uzhgorod Pipeline. (n.d.). Retrieved June 2012, from Wikipedia: http://en.wikipedia.org/wiki/Urengoy%E2%80%93Pomary%E2%80%93Uzhgorod_pipeline

Vu, K. (n.d). *Measuring the Impact of ICT Investments on Economic growth.* Retrieved Mar 15, 2014, from Harvard Kennedy School: http://www.hks.harvard.edu/m-rcbg/ptep/khuongvu/Key%20paper.pdf

Wang, W., & Lu, Z. (2013). Cyber security in the Smart Grid: Survey and challenges. *57*(5; Pages 1344-1379).

Watts, D. (2003, October 20-21). Security and Vulnerability in Electric Power Systems. *NAPS 2003, 35th North American Power Symposium* (pp. 559-566). Missouri: University of Missouri-Rolla in Rolla. Retrieved from http://cip.management.dal.ca/publications/Security%20and%20Vulnerability%20in%20Electric%20Power%20Systems.pdf

Willis . (2014). *Energy Market Review.* London: Willis Limited.

Wueest, C. (2014, January 13). *Targeted Attacks Against the Energy Sector.* Retrieved January 26, 2014, from Symantec.com: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/targeted_attacks_against_the_energy_sector.pdf

Yamane, T. (1967). *Statistics: An Introductory Analysis 2/e* . New York: Harper and Row.

Yardley, J., & Harris, G. (2012, July 31). *2nd Day of Power Failures Cripples Wide Swath of India*. Retrieved Aug 15, 2013, from The New York times: http://www.nytimes.com/2012/08/01/world/asia/power-outages-hit-600-million-in-india.html?_r=3

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

Zetter, K. (2010, Jan 28). *Report: Critical Infrastructures Under Constant Cyberattack Globally*. (Condé Nast Web Sites) Retrieved Mar 15, 2014, from wired.com: http://www.wired.com/threatlevel/2010/01/csis-report-on-cybersecurity/

Zetter, K. (2012, Jan 19). *Scada Exploits.* Retrieved August 2012, from www.wired.com: http://www.wired.com/threatlevel/2012/01/scada-exploits/

Zhao, N. (2009, Mar 23). *The Minimum Sample Size in Factor Analysis*. Retrieved Feb 11, 2013, from Encore Wiki: https://www.encorewiki.org/display/~nzhao/The+Minimum+Sample+Size+in+Factor+Analysis

Zhaoyang, D. (2014, Dec). Smart grid cyber security. *Control Automation Robotics & Vision (ICARCV), 2014 13th International Conference on* (pp. 1-2). IEEEt.

Zorz, Z. (2012, Aug 28). *Hackers allegedly breached Saudi Aramco again.* Retrieved Aug 30, 2012, from Helpnet Security: http://www.net-security.org/secworld.php?id=13493

11 PROFILE OF THE AUTHOR

V. Ananda Kumar

Anandavkumar@gmail.com

V. Ananda Kumar (Anand) is doctoral research student at the University of Petroleum and Energy Studies (UPES), Dehradun. He is the recipient of the prestigious Chevening fellowship awarded by the UK Foreign and Commonwealth Office. He has completed the PG program in Cyber Defence & Information Assurance from Cranfield University @ the Defence Academy, UK. He has done his MBA from Bharatidasan University (NIT, Trichy) and his Bachelor's Degree in Engineering form Bangalore University.

He is the General Manager, Enterprise Security Solutions Practice with Wipro Technologies. Anand is the Global Delivery Head and is responsible for technology and service delivery across application, data and Infrastructure security. He is responsible for customer project delivery, people and competency. He brings to the table an extensive understanding of the Security domains across Application, Infrastructure & Data Security domains.

Paper Publications and Seminars based on this research

1. Research Publications

- Cyber security threats in the power sector: Need for a domain specific regulatory framework in India. Published in Energy Policy Journal.

  http://www.sciencedirect.com/science/article/pii/S0301421513010471

- "Cyber Security and Culture: An Interdisciplinary Approach to Security for Cyber Security Professionals" in The Indian Journal of Criminology and Criminalistics, Jan-Jun 2015, Volume: XXXIV, Issue: 1

2. Seminars & Paper Presentation

- National Safety and Cyber Security Standards Summit April 2013

  Cyber security challenges for national critical infrastructure: Need for a policy and regulatory intervention.
- NASSCOM - DSCI Best Practices Meet, July 2013

  Making sense of the muddle – "Ways and means to realize analytics & intelligence for Cyber defense".
- Facing the reality of Cyber threats in the Power sector, Nov, 2015

  Workshop on Smart grid Communications and Cyber Security Systems at CPRI, Bangalore