Energy Policy 65 (2014) 126–133

Contents lists available at ScienceDirect

Energy Policy

journal homepage: www.elsevier.com/locate/enpol

# Cyber security threats in the power sector: Need for a domain specific regulatory framework in India

V. Ananda Kumar [a,b,*], Krishan K. Pandey [a], Devendra Kumar Punia [a]

[a] College of Management and Economic Studies, University of Petroleum and Energy Studies, Dehradun, India
[b] Enterprise Security Solutions, Wipro Technologies, Bangalore 560100, Karnataka, India

## HIGHLIGHTS

- Cyber security in power sector is key to protecting national critical infrastructure.
- Poor cyber security planning would impact the power sector in India.
- A laissez-faire approach to cyber security in power sector may not yield results.
- There is a need for power sector specific cyber security regulations.

## ARTICLE INFO

*Article history:*
Received 1 July 2013
Received in revised form
8 October 2013
Accepted 9 October 2013
Available online 31 October 2013

*Keywords:*
Cyber security regulations
Smart grid
India power sector

## ABSTRACT

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 (2012–2017). The federal government sponsored Restructured Accelerated Power Development and Reforms Program (R-APDRP) is also focused on building ICT capability in the state electricity boards. Presently however, there is no power sector specific cyber security mandates or policies in India. The Stuxnet, Shamoon and Anonymous incidents have shown that cyber attacks can cause significant damage and pose a risk to National Critical Infrastructure. A lack of security planning as part of designing the Smart grids can potentially leave gaping holes in the country's power sector stability. The paper highlights key cyber security threats across the entire power sector value chain—from generation, to transmission and distribution. It is aimed at building the case for power sector specific cyber security regulations based on the experience of regulators in other critical infrastructure sectors like Banking and Telecom in India and power sector regulations internationally.



## 1. Introduction

The Indian power sector has grown significantly from a small beginning with a miniscule capacity of 1362 MW (Indian Power Sector, 2013) at the time of Independence to 210,951 MW as of December 2012 (Central Electric Authority, 2013). 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 2010–2011. 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, 2013).

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

* Corresponding author at: College of Management and Economic Studies, University of Petroleum and Energy Studies, Dehradun, India. Tel.: +91 80 4138 1824.
*E-mail addresses:* anandavkumar@gmail.com, anandv.kumar@wipro.com (V. Ananda Kumar), kkpandey@ddn.upes.ac.in (K.K. Pandey), dkpunia@ddn.upes.ac.in (D.K. Punia).

0301-4215/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.enpol.2013.10.025

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 (approx USD 5.8 billion) in the National 12th Five Year Plan period between the FY 2012–2017 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 11th 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 (Government of India, Ministry of Finance, 2013) (approx USD 576 million) for the FY 2012–2013 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 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 to organized crime with well established market places 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 were 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, 2012), power and utilities (Brown Gary, 2011) have been the target of cyber attacks. There have been a number of international cyber security incidents like in Baltic (Tikk et al., 2012) across Estonia in 2007, Lithuania and Georgia in 2008 where the country's infrastructure has been the 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 Fig. 1.

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 the 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 of 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.

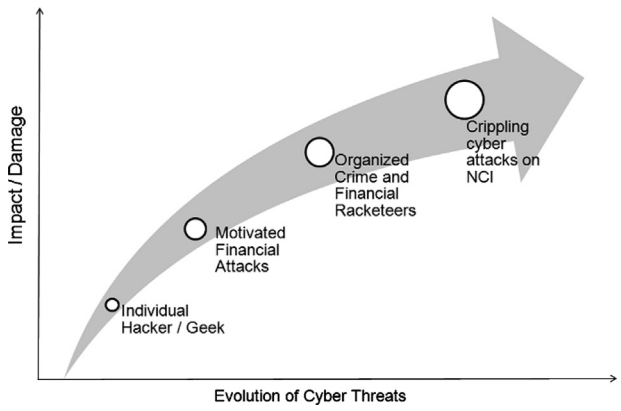


**Fig. 1.** Evolution of cyber threat and impact.

## 2. Cyber security—key challenges

As a chieftain, responsible for securing his fort in the 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 potentially 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 on 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.

### 2.1. Appreciation of the threat itself

It is easy to under-estimate the impact or damage of the cyber threat. When building applications, devices or systems the developers are focused on addressing functional requirements, non functional requirements like security are often missed out. 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.

### 2.2. 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, before it was detected in January 2007. The original breach was thought to have occurred way back in July 2005 (TJX Securities Exchange Commission Filing).

### 2.3. 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.

### 2.4. Determining the appropriate response

Organizations need to have in place an effective incident management and threat response. Whether it is responding to a credit card data loss or targeted Distributed Denial of Service (D-DOS) attack—there is need to have well structured incident response to ensure that there is business continuity and preventing a cascading effect.

### 2.5. 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 as follows:

(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 Defense—if it involves external aggressors; and
(vii) Industry players

### 2.6. Information sharing and collaboration (IS&C)

Information sharing and collaboration among the stake holders in the NCI has been almost universally acknowledged as a key component of the cyber security program. Government policy initiatives globally, whether it is the US National Cyber Security and Communications Integration Center (NCCCI) (US Cert, 2013), or UK's Cyber Security Information Sharing Partnership (CISP) (Cabinet Office, Government of UK, 2013), or India's National Cyber Security Policy 2013 (Government of India, Ministry of Communications and IT, Department of Electronics and Information Technology, 2013) all emphasize the key role of IS&C.

The US has individual sector specific Information Sharing and Analysis Centers (ISACs) and central governing National council of ISACs. In the Indian context, the CERT-In is the nodal/national level Computer Emergency Response Team (CERT) and is chartered to

- provide emergency response for cyber security incidents,
- collect, analyze and disseminate information on cyber security incidents,
- provide forensics and
- provide guidelines and advisories on cyber security.

India's National Cyber Security Policy has the stated objective of promoting sector specific CERTs that will work under the umbrella of the National CERT (Government of India, Ministry of Communications and IT, Department of Electronics and Information Technology, 2013). The Powergrid Corporation, NHPC and NTPC have been tasked to set up the sector specific CERTs in the power sector. The Central Electricity Authority has recommended that the various players in the industry, report cyber security incidents to the sector specific CERTs. The effectiveness of the collaboration within the sector specific CERTs is yet to be established, given that the sector specific Crisis Management Plans (CMPs) have still not been defined and rolled out (Government of India, Central Electricity Authority (CEA), 2013). Making the sector specific CERTs functional and effective would be key to India's IS&C program.

### 2.7. Lack of international legal framework

Given that there is today even a disagreement on how Internet Corporation for Assigned Names and Numbers (ICANN) needs to be governed—under the UN if we go with the argument extended by Indian and other Brazil, Russia, India and China (BRIC) countries or to retain status quo as argued by the 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 pinpoint 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 systems would be similar to any other and generic security solutions that work in other verticals would be well suited to address the security concerns of the power sector as well. 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 sub-segments. The subsequent section discusses the threats specific to these segments.

## 3. 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-segments in the power industry.

### 3.1. 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. Dale Peterson and his team of researchers published a list of vulnerabilities in almost all leading and widely used Programmable Logic Controllers (PLC) in January 2012 (Zetter, 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 6 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 the impact of these vulnerabilities is debatable, the point remains that an individual researcher, with very little experience on SCADA systems was within a short 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 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).

### 3.2. 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). The detailed break up is shown in Fig. 2. 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 km long and a capacity to supply over a trillion cubic feet of gas in a year (Urengoy Pomary Uzhgorod Pipeline). 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 systems 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.

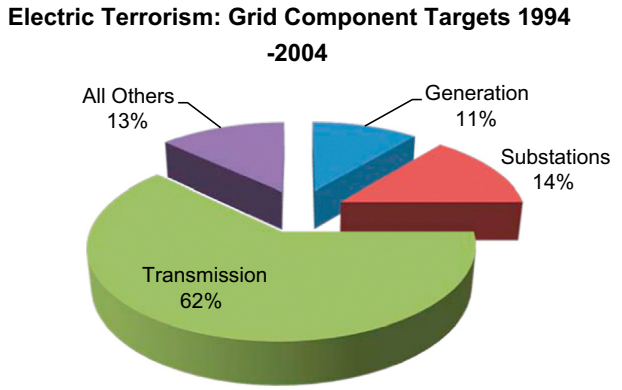


**Fig. 2.** Electric terrorism: grid component targets 1994–2004.

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 and Shukla (2012) in their research note have identified a number of 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.

### 3.3. 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 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 smart meters would cost up to USD 20 billion and 5 years of time (Anderson and Fuloria, 2012). At the basic minimum, smart meter vulnerabilities can help the consumer get away without paying for the 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, it could cause significant damage.

There is evidence to show that not all meter manufacturers have factored security into their design, C4 Security (2012), 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. 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 Erasable Programmable Read Only Memory (EPROM) dumping testing among others (Ernst and Young, 2013).

India has announced 14 smart grid pilots across the country (India Smart Grid Knowledge Portal, 2013). The 1.5 million smart meters deal to Landis+Gyr, awarded by the state of West Bengal in India (Savenije, 2013) is one of the largest smart meters deals in 2013. India must take lessons from the early roll outs in the US and other countries. One such "Epic" failure was the experience of Oncor (www.oncor.com), a utility operating in Texas, USA. Oncor procured 900,000 smart meters for deployment prior to the Public Utilities Commission (PUC) of Texas announcing the operating standards and functional requirements for smart meters. When the standards were announced, the meters were determined to be non-compliant and had to be replaced. This fiasco and subsequent settlement meant that customers had to foot a bill of USD 130 million (Flick and Morehouse, 2010). Apart from the cost, disgruntled customers can be a potential threat to the utility.

### 3.4. Threat exposure in the data connectivity (telemetry) infrastructure

A domain that is often overlooked while security planning or even while evaluating or testing the security of the cyber systems in a utility is the connectivity infrastructure or the Telemetry systems. These are the vital links that connect the control systems (or SCADA) with the various components of the electricity grid—Generation Systems, Transmission Stations, sub-stations and the consumer network. Network connectivity in a utility would include both

- "Always" connected portions of the network and
- "Intermittently" connected network segments that are used to transmit data when polled or at a specific trigger.

These connectivity links could be either Public Switched Telephone Networks (PSTN), Fiber Optic Links or over wireless like Global System for Mobile Communications/General Packet Radio Service (GSM/GPRS) or ZigBee Schneider Electric, 2013. Like any other communication systems, Power System Telemetry uses standard communication Protocols including

- Modbus
- IEC 870-5-10x
- DNP3 and
- Profibus/Profinet.

Irrespective of the type of protocol used, most of the Industrial Control System (ICS) protocols work on "Request/Response" paradigm designed for "master" (like the HMI or Human Machine Interface) to fetch data from or write into "slaves" like Remote Terminal Units (RTUs) or Programmable Logical Controls (PLCs). Most of these protocols have little or no security implementations like Authentication or Encryption (Knapp and Samani, 2013). They are thus, susceptible to malicious network attacks which can leverage the same "request/respond" implementation for "command and control" functionality. This could potentially be exploited and lead to a situation where the "slave devices" can be

- powered off;
- prevented from raising an "alarm or notification" or raise a false alarm and
- erased or cause loss of critical data.

### 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 Personally Identifiable Information (PII) 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 Call Data Records (CDR) or have access customer sensitive information, there are no such regulations in the Indian utility industry.

### 3.6. Zero days and advanced persistent threats

While Zero days and Advanced Persistent Threats (APTs) 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.

Pollet (2012) 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. This implies that there have been mission critical systems which were vulnerable to a known exploit for 3 years before the problem was found. The August 2012, Saudi Aramco breach of 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.

## 4. 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. By implementing the IT controls as part of SOX (Sarbanes–Oxley Act of 2002) compliance requirements, Industry compliance requirements like Payment card Industry Data Security Standards (PCI-DSS) 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) have driven various security implementations including Multi Factor Authentication, Application

**Table 1**
Country specific information security guidelines for power sector in EU.

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

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, 2012). This section looks at the regulatory framework in other sectors of NCI in India and power sector internationally.

### *4.1. 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 among the regulators in India when it comes to its focus on IT Security. RBI guidelines and polices on Information Security in Banking has set 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, 2012) mandating Technology and Security Standards, it continues to keep pace with evolving 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, 2012)—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% of the investments in IT Security (Symantec Corporation, 2012) 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 Unified Access Service License (UASL) mandates numerous security controls and compliance requirements on the licensee to address security needs across networks, devices, access and applications. The National Telecom Policy 2012 (NTP-2012) provides for localization and indigenous manufacture complying with specific 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 specific to the sector like control systems, distribution networks and on collaboration/information sharing.

### *4.2. Cyber security regulations and mandates in power sector in select countries across the world*

There are two different approaches to regulations in the power sector—the US approach which is largely focused on voluntary reporting mechanisms and on the other hand, EU 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 US regulations on power sector is primarily governed by the North America Electric Reliability Corporation–Critical Infrastructure Protection (NERC–CIP) mandates and the standards evolved from the National Institute of Standards and Technology (NIST) 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 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 et al., 2013).

The EU Directive includes measures to ensure a high common level of network and information security across the Union (European Commission, 2013). 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 EU directives the member states have their own internal regulatory requirement or policy guidelines or standards. A snap shot is provided in Table 1 (ENISA—European Network and Information Security Agency, 2012).

In the Indian power sector however, cyber security regulations or mandates are absent 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 and needs to be remediated.

### *4.3. 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 IT security infrastructure and processes as they need to comply with other regulations. Large utilities listed in the U.S.A 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 Gencos (Generation companies) and grid companies having to comply with these or similar norms.

### *4.4. Measuring and reporting compliance and security—metrics for NCI*

Establishing clear goals and defined thresholds are important to measure the efficacy of a cyber security program. It becomes all the more important when the efficacy of the program has to be benchmarked and compared across multiple players in the industry or signed off by the regulator. Current security metrics typically

focus on technical configuration and operational processes as a derived measure for determining the security posture. The other alternative is to establish compliance to a standard or regulatory requirement Bayuk Jennifer et al. (2012). Compliance however does not translate to absolute security, like the 2008 breach of Heartland Systems have shown (Flick and Morehouse, 2011). Security metrics are for NCI poses additional challenges as it has to span across corporate IT systems and Operational technologies. The September 2013, US GAO (United States Government Accountability Office, 2013) report on the progress of FISMA implementation highlighted two areas on metrics related improvements that could be relevant to metrics in critical infrastructure protection as well

- need for metrics to measure effectiveness of the security controls in addition to compliance;
- need to establish performance targets for metrics to measure performance over time;

The US National Institute of Standards and Technology, (NIST) has been chartered to define a framework for cyber security of critical infrastructure following the February 2013, Executive Order signed by President Obama. The draft framework is scheduled to be released late 2013.

While the NIST and other similar frameworks could provide guidance, regulators would need to ensure that the metrics are relevant to the power sector in India and there are metrics to measure effectiveness and with clear performance targets.

## 5. Conclusions

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 is 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, while in other areas such as a breach of control systems like in the case of Stuxnet it would be challenging. Security investment decisions based on ALE, would typically not address high impact but very low probability incidents. It would be very difficult of the Chief Information Security Officer (CISO) 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 Center 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 et al., 2013).

The security policy/standard for the power sector should address the entire spectrum of cyber security. 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 while we arrive at an India specific regulations for the power sector. The key components of the policy can be classified into three buckets as shown in Fig. 3.

(I) Security Policy & Standards that would be largely similar across Industries / organizations
These include
(a) Security Policy and Management,
(b) Security Organization,
(c) Security Mandates for the Corporate IT Systems,
(d) Business Continuity Planning and Disaster Recovery,
(e) Customer Data Protection and
(f) Physical Security Requirements

(II) Security Policy & Standards that would be specific to the power sector
This would include
(a) Domain Specific security standards for Control Systems.

(III) Security Policy and Standards that would be specific to the country (India)
These would be various sections that are specific to the Indian context.
(a) Periodic Assessments and Reporting,

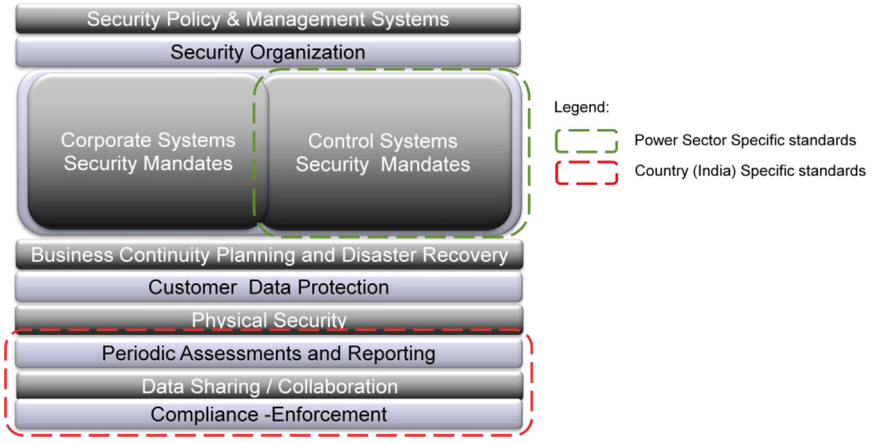


**Fig. 3.** Key components: cyber security for the power sector.

(b) Data Sharing and Collaboration,
(c) Compliance Enforcement,

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.

## References


Anderson, Ross, Fuloria, Shailendra, 2012. Smart meter security: a surver. Computer Laboratory Faculty of Computer Science and Technology. September 15, 2011. ⟨http://www.cl.cam.ac.uk/~rja14/Papers/JSAC-draft.pdf⟩ (accessed 16.06.12).

Brown Gary, D., 2011. National Defense University Press. Joint Forces Quarterly. October 2011. ⟨http://www.ndu.edu/press/why-iran-didnt-admit-stuxnet.html⟩.

Bayuk Jennifer, L., et al., 2012. Cyber Security Policy Guide Book. John Wiley & Sons, Inc, New Jersey, ISBN: 978-1-118-02780-6.

Central Electric Authority, 2013. Central Electric Authority—Monthly Exec Reports. Central Electric Authority. December 2012. ⟨http://www.cea.nic.in/reports/monthly/executive_rep/dec12/1-2.pdf⟩ (accessed 11.02.13).

Cert-In, 2011. Cert-In Annual Report 2010–11. p. 3.

Clemente, Jude, 2009. The security vulnerabilities of smart grids. J. Energy Secur. [Online] June 18, 2009. [Cited: Mar 25, 2013.] http://www.ensec.org/index.php?option=com_content&id=198:the-security-vulnerabilities-of-smart-grid&catid=96:content&Itemid=345.

Cabinet Office, Government of UK, 2013. Government launches information sharing partnership on cyber security. GOV.UK. Cabinet Office, March 27, 2013. ⟨https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security⟩ (accessed 22.09.13).

C4 Security, 2012. The Dark Side of the Smart Grid—Smart Meter (in)Security. c4-security | Resources. ⟨http://www.c4-security.com/The%20Dark%20Side%20of%20the%20Smart%20Grid%20-%20Smart%20Meters%20%28in%29Security.pdf⟩ (accessed 15.07.12).

Date, Jack, 2012. This week with George Stephanopoulos. ABCNews.com. June 27, 2010. ⟨http://abcnews.go.com/ThisWeek/cia-director-panetta-exclusive-intelligence-bin-laden-location/story?id=11027374&page=2⟩ (accessed 01.05.12).

Deng, Yi, Shukla, Sandeep, 2012. Vulnerabilities and countermeasures—a survey on the cyber security issues in the transmission subsystem of a smart grid. s.l.: River Publishers. J. Cyber Secur. Mobility I, 251–276.

Ernst and Young, 2013. Attacking the Smart Grid penetration testing techniques for industrial control systems and advanced metering infrastructure. Ernst & Young Publication. December 2011. ⟨http://www.ey.com/Publication/vwLUAssets/Attacking_the_smart_grid/$FILE/Attacking-the-smart-grid_AU1058.pdf⟩ (accessed 26.01.13).

Euractiv, 2013. EU, US go separate ways on cybersecurity. Euractiv. March 8, 2013. ⟨http://www.euractiv.com/specialreport-cybersecurity/eu-us-set-different-approach-cyb-news-518252⟩ (accessed 09.04.13).

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. European Commission, Brussels, vol. 2013/0027 (COD).

ENISA—European Network and Information Security Agency, 2012. Smart Grid Security. European Network and Information Security Agency (ENISA), Brussels.

Flick, Tony, Morehouse, Justin, 2010. Securing the Smart Grid Next Generation Power Grid Security, s.l.. Syngress An Imprint of Elsevier, Burlington, MA. (ISBN: 1597495700 9781597495707).

Flick, Tony, Morehouse, Justin, 2011. Securing the Smart Grid Next Generation Power Grid Security. Syngress An Imprint of Elsevier, Burlington, ISBN: 978-1-59749-570-7.

Government of India, Ministry of Finance, 2013. Plan Outlay—Expenditure Budget vol. 1 2012–13. India Budget. February 2013. ⟨http://indiabudget.nic.in/ub2012-13/eb/po.pdf⟩ (accessed 08.04.13).

Government of India, Ministry of Communications and IT, Department of Electronics and Information Technology, 2013. National Cyber Security Policy 2013. www.deity.gov.in. July 02, 2013. ⟨http://deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1).pdf⟩ (accessed 05.07.13).

Government of India, Central Electricity Authority (CEA), 2013. Central Electricity Authority. Cyber Threats and Security for the Power Sector. ⟨www.cea.nic.in⟩ (accessed 22.09.13).

Gross, Michael Joseph, 2011. Vanity Fair. www.vanityfair.com. April 2011. ⟨http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104⟩.

Government of India, Ministry of Communications & IT, Department of Telecommunications (Access Services Wing), 2011. Amendment to the Unified Access Service License Agreement for security related concerns for expansion of Telecom Services in various zones of the country. New Delhi, New Delhi, India: s.n., May 31, 2011.

Government of India, Ministry of Telecommunications & IT, Department of Telecommunications. National Telecom Policy, 2012. New Delhi, New Delhi, India: s.n., June 13, 2012.

Hale, Gregory, 2011. Industrial Safety and Security Source. www.isssource.com. March 23, 2011. ⟨www.isssource.com/more-scada-vulnerabilities-found/⟩.

Hoffman, David E., 2004 WashPost: CIA slipped bugs to Soviets. Industrial Defender. February 27, 2004. ⟨http://industrialdefender.com/general_downloads/incidents/1982.06_trans_siberian_gas_pipeline_explosion.pdf⟩.

Indian Power Sector, 2013. History of Indian Power Sector. Indian Power Sector. ⟨http://indianpowersector.com/home/about/overview/⟩ (accessed 11.01.13).

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

India Smart Grid Knowledge Portal, 2013. India Smart Grid Knowledge Portal. IndiaSmartGrid.org. ⟨http://indiasmartgrid.org/en/Pages/Projects.aspx⟩ (accessed 18.09.13).

Knapp, Eric D., Samani, Raj, 2013. Applied Cyber Security and The Smart Grid. Syngress, An Imprint of Elsevier, Waltham, MA, ISBN: 978-1-59749-998-9.

Langer, Ralph, 2011. TED Review—Langner—The last line of Cyber Defense. March 11, 2011. ⟨www.langner.com⟩.

Mimoso, Michael S., 2012. Bruce Schneier Reflects on a Decade of Security Trends. Bruce Schneier. January 15, 2008. ⟨http://www.schneier.com/news-049.html⟩ (accessed 01.05.12).

Malashenko, Elizaveta, Villarreal, Chris, Erickson, David J, 2013. Cybersecurity and the evolving role of State Regulations: How it impacts California Public Utilities commission. California Public Utilities Commission. September 19, 2012. ⟨http://www.cpuc.ca.gov/NR/rdonlyres/D77BA276-E88A-4C82-AFD2-FC3D3C76A9FC/0/TheEvolvingRoleofStateRegulationinCybersecurity9252012FINAL.pdf⟩ (accessed 10.04.13).

Pollet, Jonathan, 2012. Black Hat USA Electricity For Free? The Dirty Underbelly of SCADA and Smart Meters. Cupfighter. July 28, 2010. ⟨http://www.cupfighter.net/index.php/2010/07/blackhatusa-electricity-for-free/⟩ (accessed 19.06.12).

Reserve Bank of India, 2012. Internet Banking in India—Guidelines. Reserve Bank of India. June 14, 2001. ⟨rbidocs.rbi.org.in/rdocs/notification/PDFs/21569.pdf⟩ (accessed 15.08.12).

Reserve Bank of India, 2012. Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds. Reserve Bank of India. January 14, 2011. ⟨http://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WREB210111.pdf⟩ (accessed 15.08.12).

Savenije, Davide, 2013. The top 7 smart meter deals of 2013 (so far). www.utilitydive.com. March 20, 2013. ⟨http://www.utilitydive.com/news/the-top-7-smart-meter-deals-of-2013-so-far/111161/⟩ (accessed 15.08.12).

Symantec Corporation, 2012. Regulatory Compliance Drives Security Adoption in Indian Financial Sector—Symantec Report. About Symantec: Press Release. August 18, 2011. ⟨http://www.symantec.com/content/en/in/enterprise/collateral/other_resources/MediaPresentation_SymantecSecurityCheck_Indian%20Financial-Services_SurveyFindings_August18.pdf⟩ (accessed 02.10.12).

Schneider Electric, 2013. Telemetry-for-water-networks. http://www.schneider-electric.co.in. ⟨http://www.schneider-electric.co.in/documents/support/white-papers/telemetry-for-water-networks.pdf⟩ (accessed 25.09.13).

Tikk, Eneken, Kaska, Kadri, Vihul, Liis, 2012. International Cyber Incidents: Legal Consideration. NATO Cooperative Cyber Defence Centre of Excellence Talinn Estonia. ⟨www.ccdcoe.org⟩ (accessed 12.07.12).

TJX Securities Exchange Commission Filing. Form 10K of the annual report filings. ⟨http://www.sec.gov/Archives/edgar/data/109198/000095013507001906/b64407tje10vk.htm⟩.

US Cert, 2013. National Cybersecurity and Communications Integration Center. ⟨http://www.us-cert.gov/⟩. http://www.us-cert.gov/nccic (accessed 20.09.13).

Urengoy Pomary Uzhgorod Pipeline. Wikipedia. ⟨http://en.wikipedia.org/wiki/Urengoy%E2%80%93Pomary%E2%80%93Uzhgorod_pipeline⟩.

United States Government Accountability Office, 2013. Federal Information Security: Mixed Progress in Implementing Program Components; Improved Metrics Needed to Measure Effectiveness. United States Government Accountability Office. September 26, 2013. ⟨http://www.gao.gov/assets/660/658201.pdf⟩ (accessed 28.09.13).

Zetter, Kim, 2012. Scada Exploits. www.wired.com. January 19, 2012. ⟨http://www.wired.com/threatlevel/2012/01/scada-exploits/⟩.

Zorz, Zeljka, 2012. Hackers allegedly breached Saudi Aramco again. Helpnet Security. August 28, 2012. ⟨http://www.net-security.org/secworld.php?id=13493⟩ (accessed 30.08.12).