WIPRO
Applying Thought

FACING THE REALITY OF CYBER THREATS IN THE POWER SECTOR

Understanding the critical significance and need for a domain specific regulatory framework in India

www.wipro.com

V. Ananda Kumar, Dr. Krishan K. Pandey and Dr. Devendra Kumar Punia

Table of Contents

Waking Up to Cyber Threats in the Power Sector

There has been a surge in the spending in the Power sector in India with an estimated spend of USD 5.8 billion as part of the National Smart Grid Mission with the key objective of turning around India's ailing Power sector. The focus is also on driving ICT capability with the federal government specially setting up the R-APDRP (Restructured Accelerated Power Development and Reforms Program) to bring about rapid development and modernization of the State Electricity Boards in India. But the most pressing issue right now is the huge threats that cyber attacks pose for the Power sector; and there are currently no specific cyber security mandates or policies in India to thwart the eminent danger looming ahead. Designing Smart Grids without a proper security plan in place can lead to a crisis situation and result in weakening the country's Power sector stability. The paper highlights key cyber security threats across the entire Power sector value chain. It is aimed at building the case for the 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 globally.

The Need for a Strong Cyber Security Strategy

The Power sector has seen a significant growth over the years with an incredible increase in capacity - from a meager 1,362 MW at the time of Independence to 210,951 MW (as of Dec 2012). Even with this phenomenal rise in capacity over the decades, the acute problem of capacity shortage and high Transmission and Distribution (T&D) losses still persist in the current scenario. To address these critical issues, the Indian Central Government has initiated a number of structural and regulatory reforms for the Power sector. These reforms include the unbundling of the sector, promoting private sector participation, and reducing the huge AT&C (Aggregate Technical & Commercial) losses. The Smart Grid rollout in India is another key initiative towards transforming and bringing about huge changes and benefits for the Power sector.

With a planned outlay of $5.8 billion in the National 12th Five Year Plan for 2012–17, the Smart Grid Mission and the success of Smart Grid rollouts is critical to the well being of the Power sector in India. While the technology behind the Smart Grids is expected to usher in a new era, 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 security attacks as the physical world.

With the evolution of cyber threats/attacks over time, the motivation of the attackers also evolved significantly driven by financial gain - from organized crime with well-established market places for trading in malware and stolen credit card data to attacks that are designed to create mayhem and cripple the National Critical Infrastructure (NCI).

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 an increase in instances where nations' Electric Grid, Power and Utilities have been the target of cyber attacks.

This evolution brings to light the extremely worrying fact of more sophisticated cyber threats preying on vulnerable setups and systems and their impact.

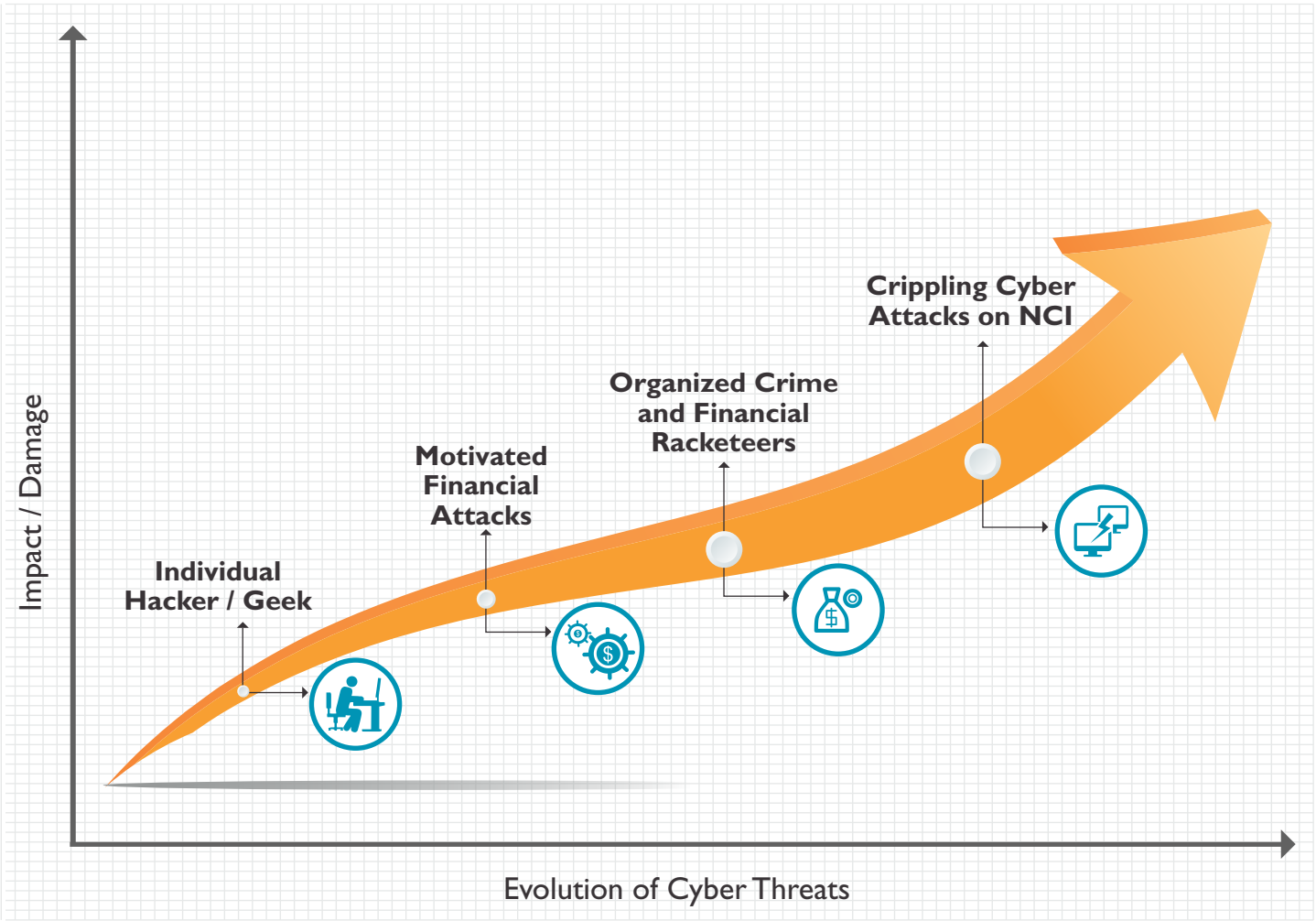

Figure 1: Evolution of Cyber Threat and Impact

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

Addressing Key Challenges of Cyber Security

The cyber route provides a perfect line of attack for potential aggressors to easily gain unauthorized access and cause unimaginable damage to the system.

This could be no different in the Indian context. This is because cyber security and response to cyber threats pose more than one challenge.

Highlighted below are a select few:

- Appreciation of the threat itself
- Challenges in the discovery of the exposure/threat
- Attribution or identifying the perpetrator or the source of the threat
- Determining the appropriate response
- Jurisdiction
- Information sharing and collaboration
- Lack of international legal framework

In the Power sector, these challenges are further compounded by sector specific nuances. Cyber security needs to be ensured across both the corporate IT systems and the Control systems. The Power sector can be broadly classified into three sub-segments – Generation, Transmission and Distribution – and security vulnerabilities exist across all the three sub-segments.

The following sections delve deeper into the threats specific to these sub-segments

Security Vulnerabilities in the Power Industry Value Chain

Conventional wisdom until a few years ago focused on cyber threat vulnerabilities on the Transmission system alone. The driving force behind this belief was that Generation systems are generally not susceptible to cyber threats since they are usually located remotely in a closed environment and are not normally connected to the Internet, and this isolation itself would make the Generation Companies (GenCos) safe from cyber threats. And at the Distribution level, the accepted view is that even in the case of a compromise or breach the impact would be minimal since the ability to damage would be localized. 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.

- **Threat exposures in Generation systems:** Numerous researches have brought to light 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.

  A team of researchers published a list of vulnerabilities in almost all leading and widely used PLCs (Programmable Logic Controllers) in Jan 2012. And by far the most well-known cyber attack is Stuxnet, which is also famous as the "Hack of the Century" or the "First Deployed Cyber Weapon in History". It is unmistakably one of the most sophisticated and most expensive malware produced. Much like a modern missile that can navigate through the air and strike at a specified target, 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.

- **Threat exposures in Transmission systems:** Historically, Transmission systems have been by far the most targeted sub-system in the Power system value chain. Over a 10 year period from 1994–2004, Transmission systems accounted for over 60% of the attacks on the Electric Grid .

Electric Terrorism: Grid Component Targets 1994-2004

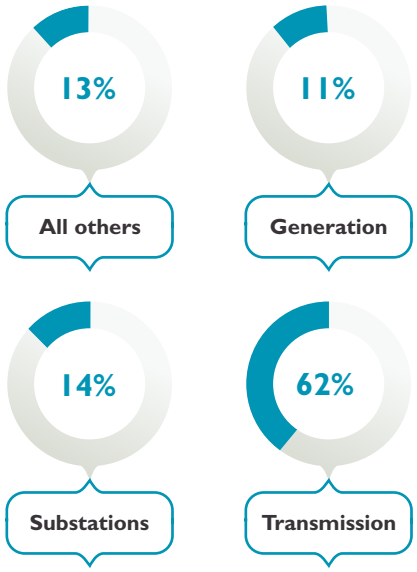

Figure 2: Electric Terrorism: Grid component Targets 1994 -2004

Many of the vulnerable PLCs affecting the Generation system and also various other cyber vulnerability exploits can impact the SCADA systems used in the Transmission sub-system. The relays on the Transmission sub-system are time sensitive and delays of even a few milliseconds can cause great damage by negatively impacting the performance and changing the desired outcome. The common Distributed Denial of Service (D-DOS) attack can flood the network and communication channel increasing the response time delays and cause the malfunction of the Smart Grids. Malicious Data Injection by compromising the Meters and introducing state estimation errors arbitrarily, which escape detection by the manipulation of the current bad data detectors, can cause serious damage.

- **Threat exposures in Distribution systems:** Smart Meter 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, it is key to introducing 'Time of the Day' billing, reducing the meter reading effort and improving efficiency.

  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 the number of units involved, which for large Utilities could run into millions of Smart Meters, security vulnerabilities post rollout would result in issues of great magnitude never seen by the Utilities.

  Patching or fixing security vulnerabilities, 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. 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.

  Leading Smart Meter brands have been found to fail in foundational security requirements including the OWASP (Open Web Application Security Project) top 10 like lack of authentication, authentication bypass, slave meter data tampering, insecure protocol implementation and 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, among others.

- **Threat exposures 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.

Like any other communication systems, Power System Telemetry uses standard communication protocols including Modbus, IEC 870-5-10x, DNP3 & Profibus/Profinet. Irrespective of the type of protocol used, most of the ICS (Industrial Control System) 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 RTUs (Remote Terminal Units) or PLCs (Programmable Logical Controls). Most of these protocols have little or no security implementations like authentication or encryption. They are thus susceptible to malicious network attacks that 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 raising a false alarm, and erased (or cause loss of critical data).

- **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 the 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, what kind of devices are being used, etc.

- **Zero Days and Advanced Persistent Threats:** While Zero Days and APTs (Advanced Persistent Threats) get the maximum coverage in the press and management attention, there are more basic issues that most security managers in Utilities need to address first.

  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 has been corroborated by studies and assessments of over 100 SCADA environments, which confirmed that 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 that were vulnerable to a known exploit for three years before the problem was found.

While a significant sum of money is 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 the 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 the one step to help attain that state.

Learnings from Other Critical Infrastructure Sector Frameworks & Global Power Sector Experience

Cyber security regulations in other (non-Power) NCI sectors in India:

While the cyber security regulation in India in the Power sector is still nascent, there is a history of cyber security regulations in other areas of NCI in India. RBI guidelines and policies 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. The Telecom sector in India has similarly seen security mandates and guidelines incorporated as part of its licensing terms for operations and policy mandates. There is therefore a precedence and significant learning that the Power sector can gain from, and focus their energy on areas that are specific to the sector.

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. Compliance however does not translate to absolute security, like the 2008 breach of Heartland Systems have shown. Security metrics for NCI poses additional challenges, as it has to span across corporate IT systems and operational technologies. The September 2013, US GAO report on the progress of FISMA implementation highlighted two areas on metrics related improvements that could be relevant to the metrics in critical infrastructure protection as well: The need for metrics to measure effectiveness of the security controls in addition to compliance, and the need to establish performance targets for metrics to measure performance over time.

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.

Other relevant IT security regulations & 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 US 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 and Grid companies having to comply with these or similar norms.

Cyber security regulations and mandates in the 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 the EU way that takes a more compulsory compliance approach with the European commission measures to ensure harmonized network and information security across the EU. 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 the need to be remediated.

Recommendations

The Smart Grid is seen as a panacea to rid the Indian Power sector of its ills, and crores of Rupees have been earmarked to achieve this goal. Upgrading the ICT infrastructure in the Power Grids without proper security planning and addressing key risks would add to the misery the industry is facing, apart from increasing the risk exposure for the NCI.

While there is certainly no lack of relevant standards to address cyber security vulnerabilities in general, 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 it would be challenging. This is aggravated further in the Indian context with the SEBs already in dire financial state.

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 figure 3 below.

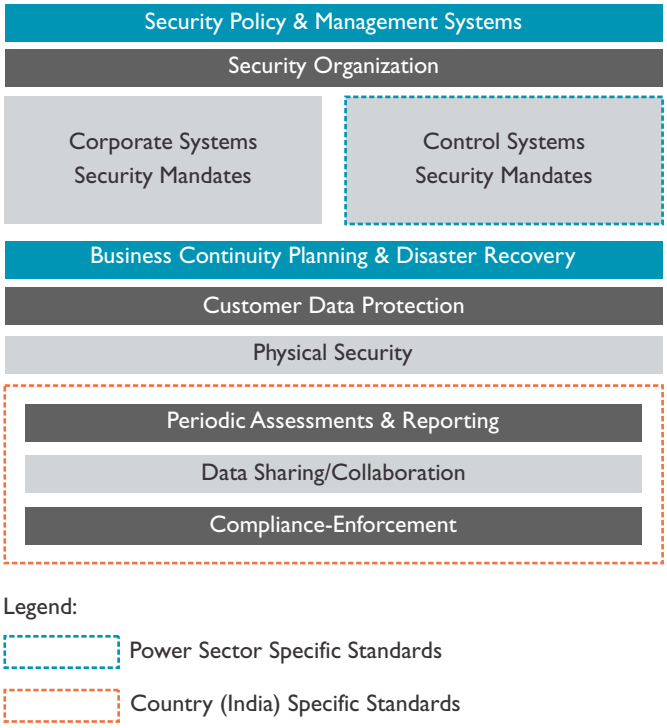

Figure 3: Key Components: Cyber Security for the Power Sector

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 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 (the Indian Computer Emergency Response Team) 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 the first step to address the cyber security issues that the Indian Power sector face.

Source

Ananda Kumar,V., et al. "Cyber security threats in the power sector: Need for a domain specific regulatory framework in India." Energy Policy (2013). <http://dx.doi.org/10.1016/j.enpol.2013.10.025>

About the Authors

V. Ananda Kumar is General Manager, Enterprise Security Solutions, Wipro Technologies and Doctoral Research Scholar, College of Management and Economic Studies, University of Petroleum and Energy Studies. He can be reached at anandv.kumar@wipro.com

Dr. Krishan K. Pandey is the Associate Professor and Assistant Dean Research, College of Management and Economic Studies, University of Petroleum and Energy Studies, Dehradun, India. He can be reached at kkpandey@ddn.upes.ac.in

Dr. Devendra Kumar Punia is Professor, College of Management and Economic Studies, University of Petroleum & Energy Studies, Dehradun, India. He can be reached at dkpunia@ddn.upes.ac.in

About Wipro Ltd.

Wipro Ltd. (NYSE:WIT) is a leading Information Technology, Consulting and Outsourcing company that delivers solutions to enable its clients do business better. Wipro delivers winning business outcomes through its deep industry experience and a 360 degree view of "Business through Technology" - helping clients create successful and adaptive businesses. A company recognized globally for its comprehensive portfolio of services, a practitioner's approach to delivering innovation and an organization wide commitment to sustainability, Wipro has a workforce of 140,000 serving clients across 57 countries. For more information, please visit www.wipro.com.

DO BUSINESS BETTER

NYSE:WIT | OVER 140,000 EMPLOYEES | 57 COUNTRIES

CONSULTING | SYSTEM INTEGRATION | OUTSOURCING

Wipro Technologies, Doddakannelli, Sarjapur Road, Bangalore - 560 035, India Tel: +91 (80) 2844 0011, Fax: +91 (80) 2844 0256, Email: info@wipro.com

North America South America United Kingdom Germany France Switzerland Poland Austria Sweden Finland Benelux Portugal Romania Japan Philippines Singapore Malaysia Australia China South Korea New Zealand

© WIPRO TECHNOLOGIES 2013

"No part of this booklet may be reproduced in any form by any electronic or mechanical means (including photocopying, recording and printing) without permission in writing from the publisher, except for reading and browsing via the world wide web. Users are not permitted to mount this booklet on any network server."

IND/RB/OCTOBER2013- OCOTBER2014