International Journal of Scientific & Engineering Research Volume 8, Issue 6, June-2017
ISSN 2229-5518

Cyber Security and Cyber Terrorism – Threat to Critical Infrastructure in Energy Sector – Challenges in India

***

Sampath Kumar V[1], Jagdish Prasad[2], Ravi Samikannu[3]

Botho University, Gaborone, Botswana, [2]Amity University, Jaipur, India, [3]BIUST, Botswana.
Emails: sampathkumaris123@gmail.com; jprasad@jpr.amity.edu; & drravieee@gmail.com

ABSTRACT

Cyber terrorism and Cyber security are two synonyms. With advancement in ICT technologies and extensive use of it in ICS in energy sector, it has its pro's and con's. Energy sector does an excellent job of managing risks facing their operations. However, cyber security and terrorism remains opaque and stubborn to monitor, manage, measure. It is critical that the environment for this be analyzed. In this paper two aspects of Cyber security and cyber terrorism is brought into limelight and discussed with a special focus and StuxNet attack which is discussed in brief. Economic impacts of cyber warfare and attacks is also discussed. Precautionary measures, defense mechanisms is portrayed.

KEYWORDS / DEFINITIONS

IoT – Internet of Things, EI – Energy Infrastructure, DER – Distributed Energy Resources; SCADA – Supervisory Control and Data Acquisition; SADC – South African Development Community; VPN's – Virtual Power Networks; PKI – Public Key Infrastructure; IDS – Intrusion Detection Systems; EMP – Electromagnetic Pulse, MTU- Master Terminal Unit; RTU – Remote Terminal Unit; ICS – Industrial Control Systems

INTRODUCTION

High speed internet connectivity has made the world a smaller place. The internet of things (IoT) has changed the way how the countries has interfaced with each other and revolutionized the business process. It has altered the way how the infrastructure is operated. This hyper connectivity is powerful tool which is an opportunity for growth in both the public and the private sectors be it Governments or Business, individuals alike. Protecting a Nations asset is critical to its management of infrastructure. Energy is essential for the development of any country and to develop its nation's socio economic conditions, be it the rural or the urban community as a whole, is an integral part of all critical infrastructure.

Technologies have their own drawbacks, benefits and liabilities. Digital technologies are transforming the way in which people interact with each other and employ machines, and how machines connect to machines. Enormous amounts of data are flowing and being stored; our world increasingly depends on the internet and digitization to be able to function. Vulnerability to theft of these data has become one of the major drawbacks of financial and other commercial transactions. The protection of data and the secure functioning of the critical infrastructure – such as energy, food and water resources, transport and communications – depend on digital technologies functioning safely and securely. Individuals' privacy in regard to, for example, medical records and insurance data is still being breached to detrimental effect. [1] Hence, Energy sector is a very vulnerable sector. An attack on this sector could throw life out of gear. So, a Nation's primary responsibility will be to protect its critical infrastructure, one of which is energy. The recent turmoil across the OPEC nations on the various fronts and challenges expose the vulnerability that the sector could go through.

With globalization, Internet has largely replaced the print media and has become a potential tool allowing effective communication. This is widely now used by terrorists or terror groups to send messages across the globe allowing them to recruit, coordinate and plan attacks evading surveillance. [2] The increasing use of internet and its inexpensive means has allowed the terrorists or terror groups to effectively bypass traditional methods of communications with dire consequences, as these impacts are largely poorly understood [3]. Differing opinions and perspectives on Nuclear energy is seen as both a blessing and curse. The concerns on health risks by radiation is very valid despite the industry's best safety and security measures to prevent any catastrophic accidents in release of radiation. However, it is a misconception that technologies are immune to any failure, accident, misjudgment or deliberate sabotage. One example is that of StuxNet worm attack on Iran's nuclear site or the Fukushima Daiichi's nuclear disaster due to the Earthquake and tsunami, which reminds us, what can be the result when protocols are compromised, be it update or upgrades [1]. The latest energy systems "Smart Energy Systems" deployed across the developed and developing nations, depended on ICT technologies, has led to exponential growth of networked intelligence in the energy sector and the consumer premises. This vast and massively expanding sector has opened up new "attack surface", which forms the backbone of the energy industry. As the energy system is fundamentally interconnected with every other critical infrastructure the cyber security threat is real. [4] The recent revelations reports on Stuxnet, Duqu, Flame, Shamoon, Dragonfly portray a glimpse of how cyberattacks is a major battle ground to gather intelligence and launch subversive activities. Most cyber weapons are low cost, but very powerful tools that can be used as both offensive and defensive tools, which can bring down a country's economy

or hold it to ransom. A major critical factor, on which security of EI depends.

Energy sector across the globe is changing fast at an unprecedented scale and pace. The need for this is due to the fact to mitigate climate change and reduce carbon print across the globe. Technologies like renewable energy system for generating electricity storage has far reaching socio economic benefits. Transformations depend on deployment of Virtual power plants, smart grids using smart technology However, these digitization strategies have both pro's and con's. All of these technologies, smart energy system is therefore created through the significantly greater use ICT digitization of energy production and distribution. The increasing decentralization of the energy system which includes consumer who is also a prosumer across the energy value chain poses a greater threat to the energy sector as a whole [4].

CYBER SECURITY THREATS AND CYBER TERRORISM IN ENERGY SECTOR

Cyber Security threat as can be defined as any *"possibility of a malicious attempt to damage or disrupt a computer network or system*". Cyber terrorism can be defined as "The politically motivated use of computers and information technology to cause severe disruption or widespread fear." An article in 2009 from the Harvard Law School on what is Cyber terrorism? There has been distinct opinions on how many of academics, politicians, security professionals etc have unanimously accepted that a common definition on Cyber Terrorism can't be agreed upon [5] Complexities of cyber threats and unknown elements, their relationships with cyber security attacks poses a challenge in defining the cyber terrorism. Although it is key to understand why the issue of cyber terrorism has been hard to explain, it is impertinent to understand if it is just a crime and it does pose a question as to when does a Cyberattack become a cyber terrorism act [6]. One report finds that US was the target in 54% of total cyberattacks in 2013, this was followed by Russia and India respectively [7]. Nearly most of the attacks originated from China while 19% of them were from US and 10% from Canada [8] [9].

Cyberattacks have many different dimensions. There are crimes where personal, financial information etc are accessed and hacked almost on a daily basis. The industrial crimes however come in different dimension, where the data is used for espionage or perhaps to bring out an industrial sabotage by breaking in corporate or government network to obtain blue prints or classified information. It is widely possible for an attacker to get inside the network and lurk for months or years scooping information of interest. In many a case, it is an insider threat due to a disgruntled ex-employee. Another category of attacks have no financial motives but just to cause terror. This categories is of greatest concern to national security officials. [10] Threats to the energy sector can be in either of the format cyber security threat or cyber terrorism. While many small scale cyber security threats are carried out on a daily basis attacks on larger scale like the StuxNet worm on Iran's nuclear facility is a classic example. This attack shows how vulnerable the energy sector is in particular to intrusion. However, there has been no record of any incident involving Cyber terrorism.

PREVIOUS RESEARCH

Notable research studies in the field energy was carried out by Kjok et.al examining the threats against petroleum infrastructure. It was implied that using ITERATE database 79% of terrorists strike against the petroleum infrastructure (between 1992-1999) was made by domestic terrorists groups [11]. Mihalka et.al made an analysis of global energy security concerns and found that despite verbal overtures by terrorists group they have not made a priority on energy infrastructure and economic targets. This was looked into more specifically after the 9/11 era. [12] Research in 2010 study on "*Terrorist targeting and Energy Security"* sought to uncover the general patterns and characteristics of contemporary terrorists attack on energy infrastructure. [13] Simonoff et.al explains in his paper that there is no correlation between energy rich countries and attacks on Energy Infrastructure and so on their ideologies making EI a priority. [14] [15]

Sporadic cyber security attacks like the Stuxnet, Shamoon across the globe in various countries, have indicated that these attacks can cause significant damage and pose a risk to National Critical Infrastructure. Thus it is essential that there be no loop holes in security planning as part of designing the Smart grids, which otherwise can potentially leave gaping holes in the Botswana's power sector stability. "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). [16]

Brazil blackout in March 1999 left nearly 70% in the dark for more than five hours affecting over 97 Million citizens. In 2003, left parts of US and Canada in chaos, leaving them high and dry without power. In matter of minutes many parts like Pennsylvania, Massachusetts, New York, Connecticut, New Jersey, Ottawa went dark. The darkness caused the public transport system to go out. Many utility corporations were shut due to this power shut down and forced emergency services like hospitals to run on limited power. [17]. Saudi Aramco was hit by a virus named Shamoom disabling over 30000 computer work stations which caused disruption for months [18]. Weeks later Qatar reported that one of their gas

companies was also affected by the same virus forcing their entire network to be offline for days [19]. Stuxnet Attack on Energy infrastructure in Iran 2010 affected SCADA systems in Bushehr nuclear power plant. This latter had affected many windows-based computers in the country. On 30th July of 2012, was an unusual Tuesday when more than 600 million people, i.e. approximately 10% of the world's population have been left without power for several hours. [20]. During 2010 a new Trojan named *Night Dragon* was injected as SQL injection targeting global oil companies. The attacks started as late as 2009 to gather information on financial information, project details in the industry. The motive was to steal the passwords, dump password hashes, sniff authentication messages and exploit the active directory configuration. [18]

According to Symantec Research Labs in 2013 parts of Austrian and German power grid collapsed after a control command was accidentally misdirected. The report also suggested that the command packet was broadcast from a German gas company to test their newly installed network branch. This transmitted to Austrian energy power control and monitoring network. It generated huge messages which generated even more data packages which inturn flooded the control network which translated as DDos attack. As a solution part of the network had to be isolated and disconnected. It was resolved without any power outages. [18]

Cyberattacks cause significant loss to Intellectual property, business intelligence, economy, can drive up cost of security, damage reputation of a company and disrupt work flow. Many companies reporting major attacks suffer a 1-5% drop in their stock value [9]. It is prudent to say while some companies may overcome these barriers, others may loose everything. Nortel Networks, a Canadian based telecom company, filed bankruptcy in 2009 when their company was infiltrated by Chinese hackers. It took several years for the investigators to discover the extent of damage to critical data [21] [9].

OBJECTIVES

The taxonomy of understanding cyber terrorism and cyber security threats in energy infrastructure is critical to the Nation's security risks at large. Hence these primary questions require to be addressed in the larger interests of the Academicians, Researchers, National Security Advisors etc in relative terms

1. Why and what are different ways of perpetrating attacks on energy infrastructure, control systems.
2. What is the Economic impact of damage and challenges in preventing such attacks?
3. What adequate precautionary measures are required and requirements needed for defense mechanisms.

METHODS OF CYBER ATTACKS

The majority of attacks on Energy infrastructure during the period 1980-2011 (8211) were classified as successful which includes the foiled attempts of 175 nos. and failed 203 attacks. 0.15% of the attacks were categorized as threats. There are numerous factors that contributed to this, which can be explained as the nature of the laying the pipelines, transmission lines, which are easy targets and highly prone. In addition to that these lines pass through many developing countries where the countries have lack of financial aids or the technology to harden their protection on the infrastructure [15].

There are numerous methods of cyberattacks noted. The attack can be on physical infrastructure or the data.

The ***physical attack*** is generally on the infrastructure. The infrastructure is damaged using conventional methods like Bombs, Fire etc. There has been little known data on these types of attack. However, the recent warfare in the Middle East and Africa has seen some of these types of attacks on the Energy sector and their take over by terrorists organizations. This *"Hostile takeover"* not only resulted in bringing down the energy prices and business but also the country's economy as a whole, thus resulting in worldwide socio-economic impacts. This type of attacks can be termed as Cyber warfare or Cyber Terrorism. Table 1 shows cyber threat matrix in energy sector.

Table 1 - Cyber Threat Matrix

Cyber Threat Matrix		
Means / Tools	Physical	Severing Cables; Bombing Infrastructure facilities;
	Cyber	Use of EMP to destabilize electronic components
Tools – Worms, SQL Injections	Cyber	Hacking into SCADA systems to control grid;
Tools – Viruses, BOTS	Cyber	Hacking into critical Government control
		Using BOTs to present inside the organizations computer network

Energy control systems comprises of different types of system critical to its functioning such as SCADA, DCS, PLC's etc. These systems are essential for generation, transmission, distribution and delivery of the energy to consumers. While

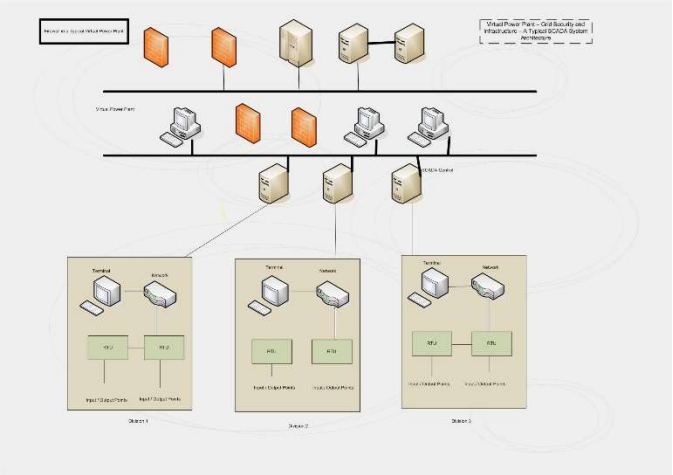

Figure 1 – A typical Virtual Power Plant – Grid Security and SCADA Architecture

SCADA provides central monitoring and control of field devices, DCS actively provides control of local processes. PLC's are small solid state devices used in both the SCADA and DC's. These systems use wide range of networking technologies to culminate data from field sites to control centres. This is a two way communication system. SCADA's (Figure 1) hardware includes different hardware components comprising of MTU's, RTU's, relays, routers, servers, workstations and display. These units run different software's like data transfer protocols, state estimators, visualization tools, reporting, equipment controllers etc. All of these hardware and software at any given point of time communicates through physical components of networking infrastructure through routers and switches either through fibre, cable or RF, microwave etc. This forms the hub of ICT infrastructure. However the difference is that most of the control systems are isolated and is separate from the ICT infrastructure [22], [23]. The computer infrastructure in case of attack becomes damaged thus modifying the control logic of the system, inducing delay and system becoming unpredictable. These types are generally known as ***Syntatic Attack*** [24]**.** The tools put to use in these cases are either virus, Trojans, or worms. The pattern of attack is unique in every attack instance.

One other type of attack known as ***Semantic attack*** is often more dangerous and damaging as it uses the human element by exploiting the confidence of the user in the system. In this form of attack the information keyed in is modified at the whims and fancies of the controller without the users knowledge to introduce errors. [24]

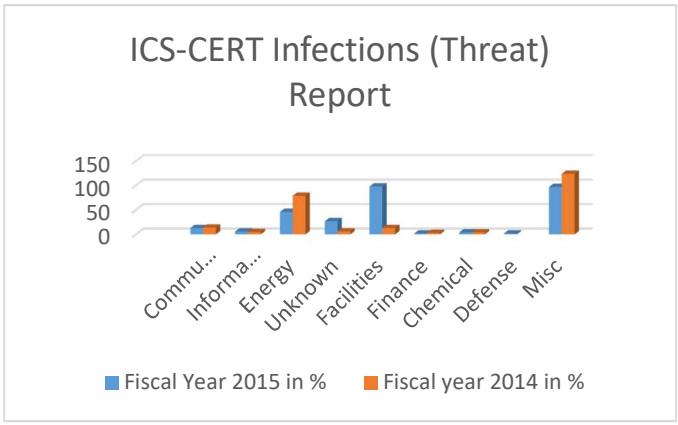

Figure 2 – ICS-CERT Infections (Threat Report) – Energy Sector – 2nd Most Targeted sector across the globe

Table 2 - ICS-CERT Report - Targets on Energy Sector

ICS-CERT Report		
Infections Reported	**Fiscal Year 2015 in %**	**Fiscal year 2014 in %**
Communications	13	14
Information Technology	6	5
Energy	46	79
Unknown	27	6
Facilities	98	13
Finance	2	3
Chemical	4	4
Defense	2	
Misc	97	124
Total	**295**	**248**

The second major threat to the Energy sector (Figure 2, Table 2) is from Cyber Security Attacks. It can be seen that nearly 80% of the attacks were targeted at Energy sector companies according to the report released by Symantec. Of these 55% involved persistent sophisticated attacks by hacktivists, insider threats and criminals. One other type of attacks was from the environment agencies and politically motivated attacks that generally contributed to bare minimum. Since various social, political, cultural dimensions form the core of these type of cyber-attacks, it is difficult to identify the key components in preventing such attacks. It should be noted that here the complexity increases as it is difficult to determine the backgrounds, behavior, motivation of the attackers. These attacks generally lead to economic impacts, misuse of power, time and money. It also affects the society and impacts it on the whole. A classic example of this can be DDos attack that was centered and directed against BARC (Baba Atomic Research Centre), Trombay. In a report by ICS-CERT [25] [26] a critical analysis on comparison of data

indicates that there has been substantial drop in the targeted energy sector when comparing it with full fiscal year in 2014. It needs to be noted that facilities includes a distribution channel. The attacks has seen an increase in the total number of Energy attacks by about 15%

Table 3 - Access Vectors (Mode of Attacks) on Energy Sector

Access Vector		
	Fiscal 2015	**Fiscal year 2014**
Miscellaneous	17	21
Unknown	110	94
Brute Force Attack	4	3
Spear Phishing	109	42
SQL Injection	4	5
Network Scanning	26	2
Weak Authentication	18	13
Removable Media	7	3
	295	**183**

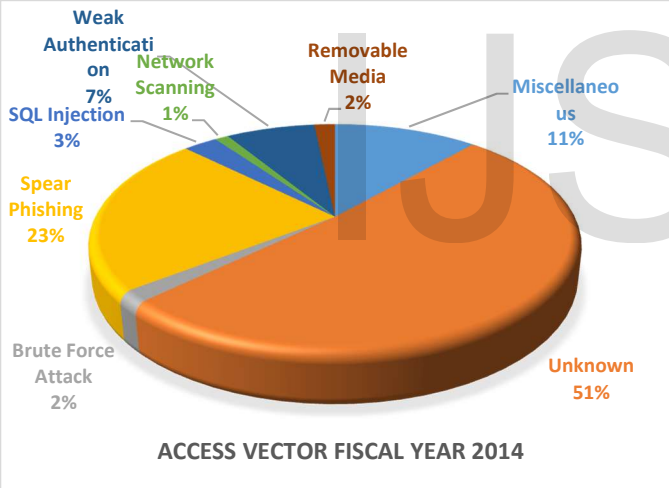

Figure 3 – Access vectors used in Cyber Attacks on Energy Sector

The mode of attacks mostly was vary from the attackers. It can be seen that during the fiscal year 2014 (Table 3, Figures 3&4), most of the attacks remained unknown with 94 (51%). In these unknown incidents it was noted that the devices were compromised in the company and was confirmed. But when doing a detailed analysis it was noted by the investigating companies that the method used to attack or intrude was not known. One important factor that needs to be noted is that either these intrusions were not detected by the intrusion prevention or detection systems or the protection was not available. It should be noted that biggest vector among the known categories is Spear Phishing with 42(23%) accounted for the most frequent method of attack.

INDIA'S CYBER SECURITY VULNERABILITIES

Most of the India's electricity system was built when technology was relatively inexpensive. The reliability on the critical infrastructure was mainly assured by having excess capacity in the system, with unidirectional electricity flow to consumers from centrally dispatched power stations or sub

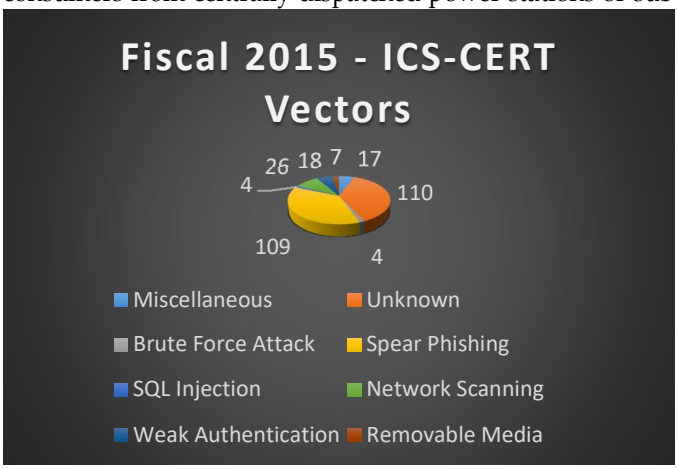

Figure 4 – Access vectors used in Cyber Attacks on Energy Sector

stations from coal-fired, hydro power plants. With the advent of green energy concept, the energy community started to combine advancements in information technology with electricity infrastructure, allowing the electric system to become "smart." The system uses interconnected elements of network infrastructure that optimizes the communications and control across the different segments of energy generation, transmission & distribution, and consumption. The brute reality is that this critical infrastructure with advancement in technology has left open a can of worms in the form of security challenges on the services it provides.

In understanding the critical security challenges and threats to India's critical infrastructure, its primary concern is espionage attacks. Attacks by GhostNet in March 2012, Navy command in 2012, IG Airport are some gentle reminders on how hackers can bring down critical infrastructure [27]. The global concerns about India's network security however, grew after June 2015 when hackers got into National Informatics Centre, thus compromising crucial sensitive data. The mode of this attack went undetected for months. Government of India which ran a survey through its nodal agency indicated that over 780 attacks damaged several computers in 88 cities and over 350 hacking attempts on sensitive computer systems [28] [24].

The global data on the cyber security attacks on IT infrastructure from July 2012 to 2013, on an average had about 74 targeted attacks per day globally. Of these 8-9 attacks were on energy sector alone accounting for the second most targeted system, accounting for 16.3 percent. In a report released by Symantec in March 2015 indicated that almost close to about 80% of the attacks in the sector in the globe was targeted at energy sector companies. Of this 55% involved advanced persistent threats carried out by sophisticated hacktivists, insider threats and Criminals. The last few years have seen an exponential growth of threats. In

its Quarterly report Symantec 2015 threats no of breaches increased 23% from the previous report for 2014. MacAfee says that the malware intrusions increased by 50% than the previous years. As the complexity of the cyber security increases so do the threats.

The StuxNet worm (Fig 5) was first discovered by Kaspersky Labs on a request from a Belarusian company on behalf of Iran's Nuclear Agency. Stuxnet "showed that it was perfectly possible for a cyber-attack to result in significant physical damage to energy infrastructure as well as the ensuing consequential/business losses". [29]. This was designed to spy on the industrial control systems. It was also capable to cause the centrifuges to spin out of control and tear themselves apart. In India it affected close to about 10% of the systems across the country running Siemens SCADA. The Target in this case was only the Simens controlled SCADA systems.

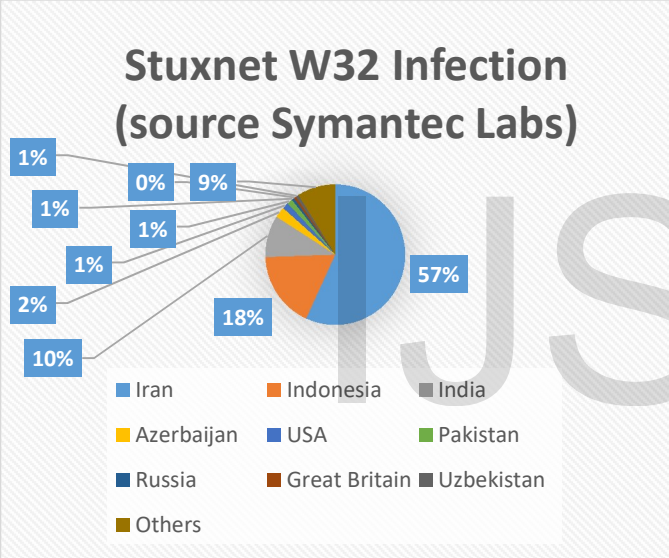

Figure 5 – StuxNet Infection during 2010 Attack on CIS

ECONOMIC IMPACTS

Any threat on the energy infrastructure will have impending effects on the economy. It will translate to losses. The losses can be substantial which could result in business disruption, loss of time and money and damage to reputation. On a financial side, the results will be on downtime, productivity loss depending on the attack mode or where the attack is centered, it could be anything ranging from application level vulnerabilities to targeted segment. The economic impact of any form of attacks has it is own consequences the same is applicable in case of cyberattacks and cyber terrorism. It will have many dimensions and aspects with impact on society, organization, individual etc. Many countries spends a major chunk of their budget in fighting with crimes. India is no exception to it. With the IT infrastructure adding to the list of the Country's Budgets, "it means that along with the security of this country's nationals, now humongous amount of resources have to be invested in cyber security as it is a threat of an equivalent magnitude of risk. The major challenging economic consequences of cyber-attacks are budget constraints, and resource limitations". [30] "asserts that most law enforcement agencies are presented with funding as a critical challenge. Furthermore, the investigation resources like sufficient manpower to be employed in case of a cyber-attack are always limited. The economic impacts on these attacks have significant impact on the economy as a whole." Tackling cybercrimes and cyber-attacks on the energy sector poses significant challenges on its own. The most important of this cost of these attacks comes from its damage to company's performance and to the national economies. It impacts trade, competitiveness, innovation, economic growth, GDP etc. The cost of cyberattacks will continue to increase as more and more business functions are computerized.

Cyberattacks is a tax on innovation and slows down the global research and innovation reducing the rate of return to investors and innovator. While Government's across the globe begin serious and systematic efforts to collect and publish data on the cyberattacks to help countries and companies fine tune their risk and help in analysis about potential risks, it has numerous snags and challenges on many fronts. According to many Security companies, very few companies are willing to share their attacks patterns on their infrastructure. It simply means that any dollar amount (Costs) for global cyberattacks is only an estimate based on incomplete or non-reliable data. It is also true that few nations have made serious efforts to calculate their losses from the cyberattacks, most have not. India is no exception. The primary reason being "fear of exposure" will lead to company's finances being hit. With companies in India facing global challenges on the protecting it security in infrastructures due to myths that any exposure could lead to larger financial impacts, very few companies even come forward to publish their data that there was a potential breach in the security.

Table 4 - Economic Impacts - in Millions($)

	USA	Germany	Japan	UK	Brazil	Australia	Russia	India
2014-2015	15.42	7.5	6.81	6.32	3.85	3.47	2.37	4.44
2013-2014	12.69	8.13	6.91	5.93		3.99	3.33	4.4
2012-2013	11.56	7.56	6.73	4.72		3.67		4

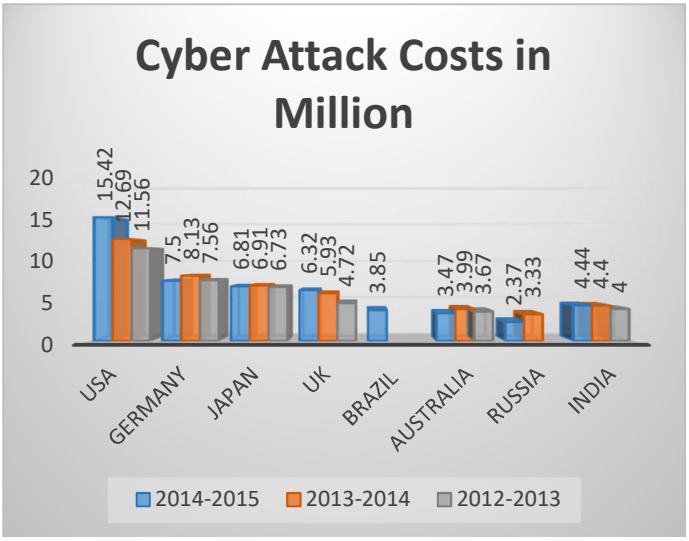

Figure 6 – Economic Impacts – Costs in Million ($)

According to latest research by Ponemon Institute in collaboration with HP, It was noted that the cybercrime has increased considerably when compared to the previous years. Energy infrastructure is still the potential leading sector, next only to financials, in terms of attack. [31]

It is noted from the above table 4 that the "Identified target firms have to suffer 2% – 10% of losses in days after an attack when translated in money terms would account to about $100 million to $200 million". According to McAfee report 2015 [32] the losses ranged from $15 billion to $1 Trillion due to various attacks (figure 6). Computer security consulting firms, that generally compile these figures, often fail to consider the numerous number change that depends on the nature of attack on the focused firm, it is important to note that the spiraling costs on the cyber security is impacting the economies in many countries.

PRECAUTIONS, DEFENSE MECHANISMS

Considering the impact of the Cyber terrorism and Cyber threats it is essential that proper precautionary measures and defense mechanism to be employed in protecting the critical infrastructure of the Nation. Careful strategies are required to mitigate the impacts of threats in the form of Cyber Terrorism and Cyber Attack. Historical data and well documented data can be used as metrics to analyze and provide necessary solutions. Hence it is essential that a private-public partnership is critical in documenting the disasters. Since cyber security is a complex issue, it is understood only by a small fraction of secluded individuals or cadre, it is essential that participation and training in terms of handling needs security needs to be driven down the chain to the lower level. Therefore it is critical to apply risk management principles that have worked well. The first ones that are attacked in case of cyberattack is the computers. A compromised computer can be source or platform for the attacker's entry into the network of system to explore deeper. Therefore it is essential and critical to secure and harden the Operating System with constant updates and patches. Recurrent awareness trainings be carried out to help users identify social engineering attacks like BOT's etc to help them from being a victim. Frequent penetrating testing can be made using sophisticated software's to access vulnerability. This will help access the application against SQL injections and other forms of web attacks. Frequent updates and Patches should be made on the software's. Latest information on Trojans, Viruses etc should be circulated to create awareness among the employees. Filtering the network traffic with sophisticated firewalls, content filters, intrusion prevention allows the control of data flows. This will also help in monitoring the data both inwards and outwards. This will be a key point in keeping cyber espionage at bay. Endpoint protection can be applied to all IT devices to protect from viruses and worms. ICS; PLC's, SCADA etc are non standard IT systems. These needs to be hardened with the increase in security. This can be done through effective policies, constant upgrade of firmware etc. Hence it is essential that the lockdown tools can be used in protecting these critical infrastructure. While in most cases PLC's, SCADA systems are on the isolated network it is essential to ensure that it is has redundancy and failover protection. Authentication using hardcoded passwords, PKI's, Biometrics should be used in critical areas or key areas. The passwords etc should be changed regularly and should adhere to password policy. Strong passwords should be made mandatory. Since most industrial controlled systems have weak authentication it needs to be substantiated with other security mechanisms where applicable. Although many industries use VPN, it is essential that the traffic in them be monitored to prevent any unwanted attack.

RESULTS, DISCUSSION, CONCLUSION

Cyber terrorism, espionage are becoming increasingly common. The threats are real with countless actors attempting to gain entry into some of the best practiced and protected systems in the energy sector. Roughly about 4-5 attacks takes place on a regular basis in the energy firms with increasingly sophisticate technology with varying degree of threats and tactics. From 2009-2015 observations indicate that energy sector has moved up from being low down the top list to become the second most targeted sector. In India the energy sector is very vulnerable. Most of the energy attacks translate to gathering valuable information rather than being an act of cyber warfare or cyber terrorism. Although the attackers have been focusing on gathering information a day is not far away when these attacks will be to sabotage, leading to huge financial losses. Energy firms need to be aware of these risks to protect their valuable information as well as their ICS or SCADA networks.

In many a case, Cyber security is regulatory compliance issue for many businesses. They need to ensure that they are

protected adequately from cyber risks. It is therefore critical for the businesses to know what their obligations, responsibilities are and they need to comply with it. Cyber-attacks and risks should be made mandate for them to disclose as part of business risks. This may help in assessing how exposed their business are and then what precautionary measures need to be taken to protect their business and their investors interests.

Bibliography

[1] Caroline Baylon, Roger Brunt, David Livingstone, "Cyber Security Threats at Civil Nuclear Facilities - Understanding the Risks," Chatham House, London, September 2015.

[2] Max Roser , Mohamed Nagdy, "'Terrorism',," 2016. [Online]. Available: https://ourworldindata.org/terrorism/. [Accessed 02 3 2017].

[3] B. Hoffman, "Inside Terrorism," Columbia University, 2013.

[4] David Healey, Sacha Meckler, Usen Antia, Edward Cottle,, "Cyber Security Strategy for the Energy Sector," Eurpoean Union, Brussels, 2016.

[5] Victoria Barnetsky, "What is Cyber Terrorism; Even the Experts Cant Agree," The Harvard Law Record, 2009.

[6] Sam Powers, "The threat of Cyber Terrorism to Critical Infastructure," New York University, New York, 2013.

[7] Verizon, "Data Breach Investigations Report," Verizon Group, 28 Nay 2014.

[8] "Fourth Quarter 2014: State of the Internet," 2014.

[9] Bryan Watkins, "Impact of Cyber attacks on the private sector," MidPoint Group, 2014.

[10] Peter Maass, Megha Rajagopalan, "Does Cyber Crime Really Cost $ 1 trillion," ProPublica, 2012.

[11] Ashild Kjøk & Brynjar Lia, "Terrorism and Oil – An Explosive Mixture? A Survey of Terrorist and Rebel Attacks on Petroleum Infrastructure 1968-1999.," 2001.

[12] Michael Mihalka, David Anderson, "Is the Sky Falling? Energy Security and Transnational Terrorism, Strategic Insights`," *Center for Contemporary Conflict at the Naval Postgraduate School*, 07 2008.

[13] John C. K. Daly, "Saudi Oil Facilities: Al-Qaeda's Next Target?," *Terrorism Monitor 4,* vol. 4, no. 4, 2006.

[14] S.J. Simonoff, C. Restrepo, R. Zimmerman & E.W. Remington, "Trends for Oil and Gas Terrorist Attacks," I3P, Hanover, November 2005.

[15] Jennifer Giroux, Peter Burgherr, Laura Melkunaite, "Research Note on the Energy Infrastructure Attack Database (EIAD)," *Prespectives on Terrorism,* vol. 7, no. 6, 2013.

[16] Anand Kumar, Dr Krishnan Pandey and Dr. Devendra Kumar Punia, "Facing the Reality of Cyber Threats in the Power Sector,," *Energy Policy,* vol. 65, pp. 126-133, 02 2014.

[17] CIP Center for Infrastructure Protection, "A case of study of the 2003 north American blackout with exercice," 2003.

[18] Candit Wueest, "Targeted Attacks Against the Energy Sector," Symantec Labs, 13 January 2014.

[19] KPMG Global Research Institute, *Energy at Risk,* KPMG, 2013.

[20] Benahmed Khelifa, Smahi Abla, "Security Concerns in Smart Grids: Threats Vulnerabilities and Countermeasures," in *Renewable and Sustainable Energy Conference (IRSEC), 2015 3rd International*, 21 April 2016.

[21] Siobhan Gorman, "China Hackers Suspected in Long-Term Nortel Breach," *Wall Street,* 14 Feb 2012.

[22] Terry Fleury, Himanshu Khurana, Von Welch, "Towards a Taxonomy of Attack agaist Energy control system," in *University of Illinois at Urbana-Champaign*, Illionis.

[23] Keith Stouffer, Joe Falco, and Karen Scarfone, Guide to Industrial Control Systems Security Recommendations of the National Institute of Standards and Technology, vol. Second Public Draft, NIST Special Publication 800-82, September 2007.

[24] Amar Singh, "Spectre of Cyberterrorism: A Potential Threat to India's National Security," *Indian Journal of Research,* vol. 5, no. 3, 2016.

[25] ICS-CERT, "Year In Review," Homeland Security, US, 2015.

[26] ICS-CERT, "Year in Review," Homeland Security, US, 2014.

[27] Omair Anas, *"In search of India's Cyber Security Doctrine",* New Delhi: Indian Council of World Affairs, 2015.

[28] Staff Correspondent, *Centre to Shield India from Cyber Attacks Proposed,* New Delhi: The Hindustan Times, 2014.

[29] David Kushner, "The Real Story of Stuxnet,," *IEEE Spectrum Posted,* 26th February 2013.

[30] F. Lemieux, *Investigating Cyber Security Threats,* Cyber Security Policy and Research Institute, George Washington University., 2011.

[31] Ponemon Institute, LLC., "State of IT Security: Study of Utilities & Energy Companies.," Ponemon Institute, LLC. ., April 2011.

[32] Carlos Castillo, Diwakar Dinkar, Paula Greve, Suriya Natarajan, François Paget et.al, "McAfee Annual Lab Reports," McAfee, November 2015.