Vol. XIII & Issue No.12 December - 2020
INDUSTRIAL ENGINEERING JOURNAL

ASSOCIATED THREATS OF INDUSTRIAL CONTROL SYSTEMS AND AWARENESS OF CYBER SECURITY IN ENR SECTOR OF INDIA – A CASE STUDY

Mahesh Singh
Dr. Kishore K. Morya

Abstract:

Connecting everything to the Internet is the discussion across the globe today. Near future will be of the fourth industrial revolution, where cyber-physical systems, the Internet of Things (IoT) and Internet of Services (IoS), are more significant to OEMs, system integrator and asset owners. Thus, it is only a matter of time when maximum ICS information is routed to sophisticated applications across enterprises through a wide area network where security is insignificant leading to ineffective protection. Convergence of Operation Technology (OT) with external networks and the Internet is opening several connections and is being managed over handheld mobile devices held by system administrators. Therefore, it has become vital to get the OT systems within the purview of cyber security to make them secure. As the Energy and Natural Resources (ENR) Sector too are now deploying advanced automation for considerable bottom line developments during convergence of Information Technology (IT) and Operational Technology (OT), which has made these organisations susceptible to frequent cyber-attacks, it brings more focus towards OT as well. Now, it is inevitable for organisations to come together and to take cognizance of the current dynamic cyber environment and take proactive actions accordingly. The ENR Sector being the most important sectors in the economy of any nation, the impact of cyber-attacks in this sector is widespread for any organisation and may even have worldwide political and commercial effects in certain cases. This paper highlights the cyber risks faced by Industrial Control Systems, awareness of Cyber Security of Operational Technology (OT) in ENR Sector in India and gain insights into their peers, as well as boost their preparedness to reduce the risk of cyber-attacks.

Keywords: Energy and Natural Resources (ENR), Information Technology (IT), Operational Technology (OT), Industrial Control systems (ICS), Supervisory Control and Data Acquisition systems (SCADA), Cyber-attacks, Critical Information Infrastructure (CII).

1. INTRODUCTION

As defined by Graham Williamson [1], Operation Technology (OT) represents industrial control systems (ICS) and Supervisory Control and Data Acquisition systems (SCADA) of an organisation. Operational Technology (OT) talks about computing systems that are used to accomplish industrial operations in contrast to administrative operations. Operational systems comprise of production line management, oil & gas monitoring, mining operations control etc. Industrial Control Systems (ICS) include systems that are used to monitor and control industrial processes and are a major part within the Operational Technology segment. Examples of ICS include mine site conveyor belts, oil refinery cracking towers, power consumption on electricity grids or alarms from building information systems, etc. ICSs are usually used in mission-critical applications with a high availability as prerequisite [1]. Most ICSs are of two types either a Continuous Process Control System, managed via Programmable Logic Controllers (PLCs), or Discrete Process Control Systems (DPC), that might use a PLC or some other batch process control device [1]. Industrial Control Systems (ICS) are managed via a Supervisory Control and Data Acquisition (SCADA) systems that provides graphical presentation of events, logs alarms of field devices and user interface for operators to manage the process under control.

Historically, most of these control systems operated in isolation with proprietary technologies. Accordingly, cyber-security risk from external attackers was limited. However, nowadays, transformation and the adoption of existing commercial technologies led to these systems becoming increasingly connected and interdependent [2]. Standard SCADA implementation of traditional isolation architecture might look like Figure 1.

1.1. Statement of the problem

As ENR Sector across India digitalise at a rapid rate by integrating Industrial Control Systems (ICS) with corporate network and Internet for business requirements, the cyber security frameworks do not necessarily develop at the same pace, which has left many firms vulnerable to attacks in the digital domain. This led to study of this sector to provide insight for emerging cyber threats and readiness to cope up with these attacks.

1.2. Research objectives

- The study is aimed to know various cyber risks faced by ENR Sector in India.
- The specific objective is to analyse the level of preparedness of organisations to deal with cyber security threats in the sector.

2. LITERATURE REVIEW

2.1 Impact of Cybercrime in India

It is reality that most of the world not prepared well to handle Cybercrime. It is unpredictable, often undetectable and has unrestricted reach due to which a hacker in one corner of the world can break into a system at other corner easily which

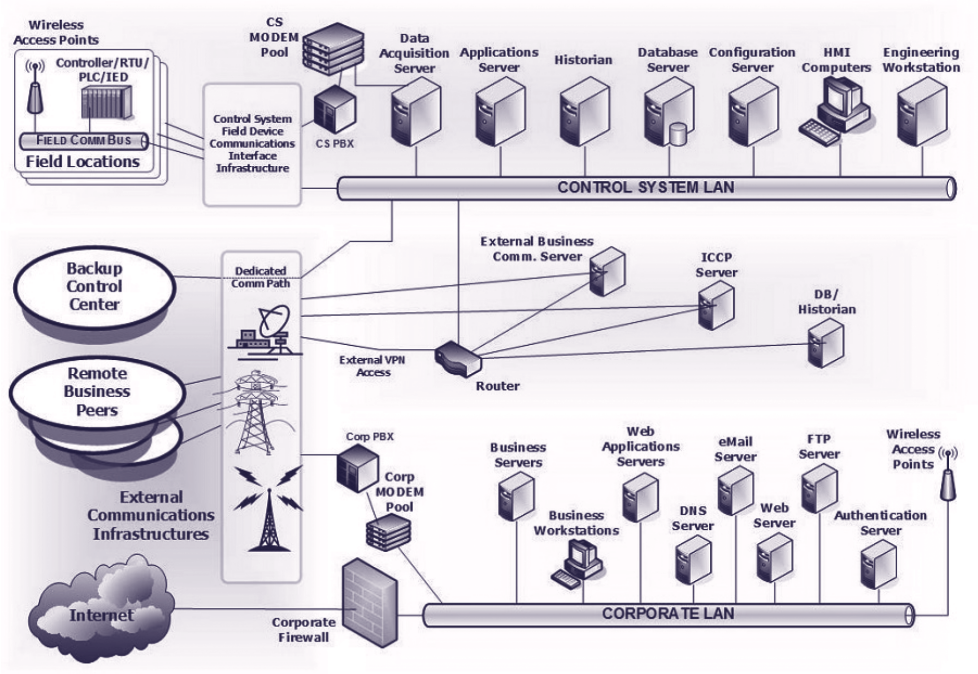

Fig. 1. Traditional isolation of corporate and control domains. [3]

can create jurisdiction problems to handle. Consultancy India reported on its website on June 4 2018[4], "As India digitises, cybercrime is becoming an increasingly tangible threat", India ranks quite high on the worldwide list level of cybercrime as well. By the percentage of criminally controlled systems as a metric, the United States is at the top most affected by cybercrime at 23%, followed by China at 9%. Germany, Britain, Brazil and Spain follow with between 4% and 6% each. Though India registers 3% of criminally penetrated systems, the country ranks third in terms of the entire number of systems affected. The increase in cybercrime will definitely affect ENR Sector of India as this sector has too been digitised considerably.

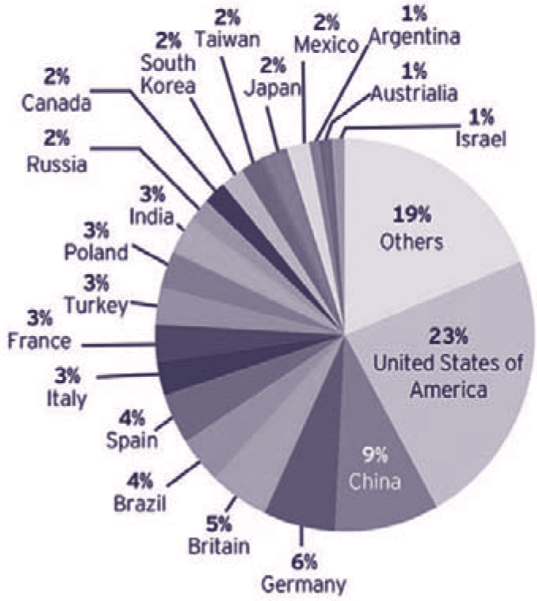

Fig. 2. Global impact of cybercrime [4]

2.2 Associated risks of an organisation

As per Risk Survey conducted in 2018 by Deloitte "Transforming Risks into Opportunities" [5] Cyber Security, Technology Disruption, and Regulatory Risks are the top 3 risks impacting any establishment both in the present day situation and in future as well. However, the emphasis on Cyber Security and Technology Disruptions is estimated to deepen in near future, while Regulatory Risks appears to follow a falling trend.

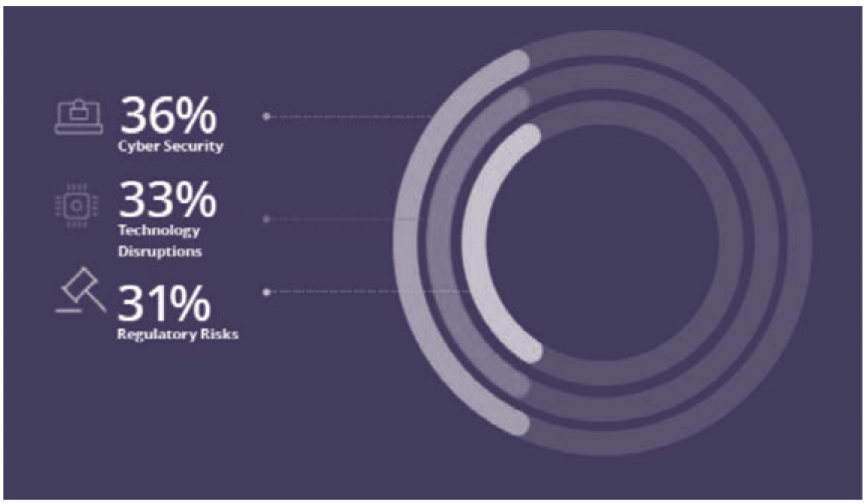

Fig. 3. Associated risks of an organisation [5]

2.3 Security threats associated with critical infrastructure

As ICS gradually being converged with the corporate network and Internet to address business requirements, it is obvious that sector is exposed itself to the world of attackers. This is apparent from many global information security surveys, such as ICS-CERT [6]. Figure 4 below highlights that almost all critical infrastructures are targeted.

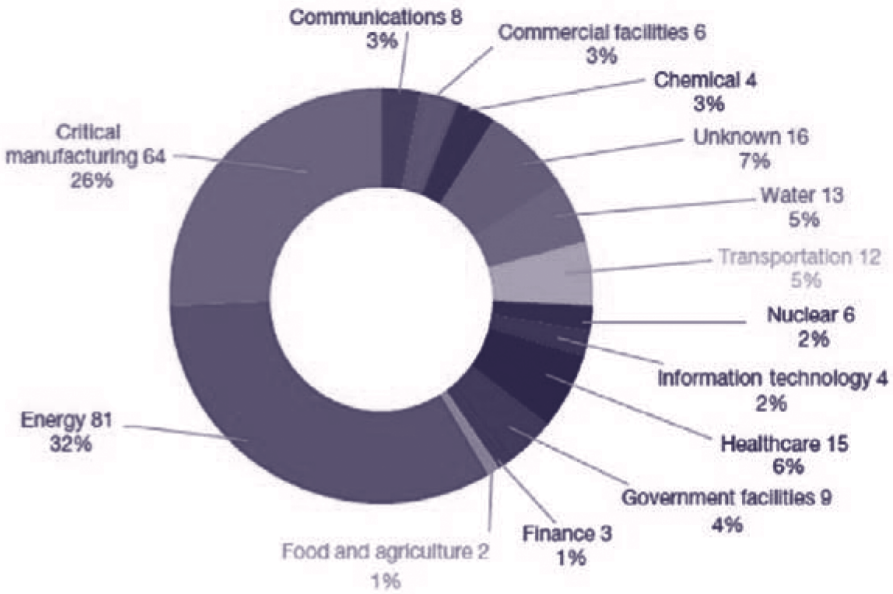

Fig. 4. Security threats associated with critical infrastructure. [6]

As per Indian Computer Emergency Response Team (CERT-In), the number of incidents reported till June 2017 was 27,482. Cyber threats becoming more refined and resourceful, the effect of cybercrime is increasing, and the attacks are increasing in volume and variety as well. "India was the third worst affected by WannaCry (an advanced ransomware attack) among more than 100 countries those were hit" [7].

2.4 Various Security weaknesses of ICS

Use of legacy devices and software in most ICS environments is the main reason of security flaw. Security developments and system upgrades of ICS environments have deferred due to difficulty and cost of mitigating ICS security. K. Stouffer, J. Falco, K. Scarfone, "Guide to Industrial Control Systems (ICS) Security", NIST Special Publication (SP) 800-82, deliberated challenges to ICS and few of them are illustrated below [8]:

2.4.1 Convergence of IT and OT

Integration of modern ICS with corporate LAN for remote monitoring and control and allowing remote access of ICS to vendors and support personnel, these rights of access to ICS invite many openings to breach security. Few areas of flaws are deliberated as below:

- **Denial of Service (DoS) attacks**

Invalidated sources and incomplete access controls permit attackers in damaging OT systems to perform DoS attacks on susceptible unpatched systems. ICS are exposed to commonly known TCP/IP DoS attacks like SYN flooding, low-rate DoS (LDoS) attacks manipulating TCP's retransmission time-out mechanisms, or buffer-overflow scenarios. In fact, DoS can be achieved by just sending reset, halt, or reboot commands. Even block encryption or port-scanning tools of conventional IT security can "freeze up" or considerably make slow control systems, causing in DoS [8], [9].

- **Use of outdated and open source protocols**

ICS operations typically use obsolete, insecure protocols such as FTP and Telnet. Modbus/TCP, Ethernet/IP and DNP3 SCADA communication protocols of ICS for control devices normally do not require any validation to remotely execute commands on a control device, and no encryption alternatives available [10], [11].

- **Absence of Basic access control implementation**

Most devices require most elementary access control isolating framework software mode versus application program mode. Server and terminal validation is either not exist or entirely useless. Distinction of access rights among administrators and end users is usually absent or not employed [9].

- **Man-In-The-Middle Attacks**

Network intruders can manipulate in-transmission directions, commands, or alarms due to absence of encryption and mutual authentication of ICS. Reiteration bouts can activate automatic system reactions causing in erratic malfunctions. Prompting system operators to take wrong and possibly risky human intervention due to wrong monitoring data presented by spoofing bouts. Network sniffing may expose secret data to invisible seizure for governmental or industrial spying, radical attacks, or felonious chases [8], [10].

- **Corrupted Control System Device**

Control logic software is not secure and can be effortlessly changed. Corrupted devices can end in system damage, interruption, or safety hazards. Firmware is not secure, making it possible to alter configuration settings or push malevolent code over Ethernet in many cases. Subsequent device failure or unpredictable functionality may result in DoS events [9], [10].

2.4.2 ICS Configuration Issues

There is always vulnerability to the security while deployment of ICS with industry standard hardware and Operating Systems (OS) still these systems deployed with least security technologies and practices. Most common reason is default services and out-of-date software [8], [9].

- **Default configurations for unwanted services**

Outdated systems with default or week passwords and standard configurations make it easy for attackers to tally and intrude in OT systems. Various processor and network services run in default mode in open source OS platforms. Due to this unmonitored exposed ports prone to network abuses and aggressively implementing code that may result to buffer-overflows attacks [8].

- **Operating system, malware protection software, or security patches outdated**

OT Systems run on legacy software that lack sufficient user and system authentication, data authenticity verification, or data integrity checking features that allow attackers uncontrolled access to systems. Comprehensive testing of software and security update require due to high availability and critical latency. These actions need to plan well in advance but rarely allowed that too for short duration. Secondly, due to criticality of low latency in ICS mechanisms security software are usually allowed. This leads to obsolete OS levels and old-fashioned or no malware defence software. In short, even if antivirus software is updated, ICS is further vulnerable to new malware due to its standard platform and can't be further patched timely [8], [12].

- **Retrofitting additional hardware and software**

Response time of network increases by retrofitting typical IT security tools into a control system. This delay may introduce operational errors in the system, or cause the system delay or complete failure. Only vendor approved changes to be allowed such as installation of software or with the control system. Application of any ad hoc security tool is allowed into ICS environments only when overall performance testing to ensure actual performance requirements has been done [9], [11].

2.4.3 Absence of Audit and Control Procedures

Traditionally, ICS system works in isolated environment where all communications were trusted and the priorities of ICS processes were safety, availability and response time. Operational security management or techniques, audit procedures, or computer forensic data were not essential.

- **In adequacy of Security policies and Cyber-criminal data**

Various legacy devices not have required logging capabilities. Logging capabilities may not be configured properly or monitored for abnormalities that are present [9], [13].

Due to complex external connectivity, ICS systems are vulnerable to security bouts which were not considered when the systems were originally designed. There is gap between development of security policies for the ICS and increasing experience to cyber threats [13].

- **Failure in detection of Incidents**

Online monitoring tools are absent or not configured effectively. Events that are present may be ignored due to absence of proper monitoring measures [8].

2.5 Significance of ICS cyber security globally

Most of organisations prioritise cyber security of OT/ICS as one of the main focus area. The risks are understood therefore framework for actions is ready. Based on survey conducted by Pierre Audoin Consultants (PAC – a CXP Group Company) with 320 worldwide experts in decision making authority on OT/ICS cyber security, Kaspersky lab published a report in June 2018[14]. The survey revealed that 77% organisations of opinion that cyber security is major risk and is in major priority list.

2.6 Cyber risk awareness level in ENR sector

Cyber security of ICS systems is of utmost importance as cyber-attacks will increase in frequency, severity and impact year after year. As per survey conducted on "Cyber security survey - Operational Technology Energy and Natural Resources" by KPMG in India [15] of the prominent ENR companies in India to determine their risk awareness and security practices of Indian corporates in the Energy Sector which are summarised below:

- Organisations that have OT security team that support well-defined cyber security policy for OT setup are only 27%.
- In71% organisations security posture of OT based on reports provided by external auditors and SMEs.
- 31% organisation's OT systems required software patching.
- System should be more secure by OEMs for competitive business as per 39% organisations.
- 38% organisations feel that OT atmosphere is on major risk as OT support team has inadequate skills on security.
- 31% organisations are required to be associated with sectoral CERT & NCIIPC.
- 54% management believes that an integrated robust policy formulation is required covering critical infrastructure sector.
- 31% organisations feel that support on cooperation and knowledge sharing on cyber incident is vital amongst peer organisations to develop the cyber security posture in the OT atmosphere.

From the literature review it is evident that increased digitisation is the main cause of vulnerability to ICS which needs to be addressed appropriately to avoid disruption in the operation of critical infrastructure.

3. KEY CYBER SECURITY INITIATIVES LAUNCHED IN INDIA

India ranked 5th in 2015, according to the International Telecommunication Union's (ITU) Global Cyber Security Index but has come to the 23rd rank in 2017 among 134 countries [16]. By learnings from other nations and with solid initiatives, the security scene of the country may be further improved. As progressive country, some initiatives have been taken by India to strengthen its cyberspace. Few of the significant initiatives are stated below:

- **National Cyber Security Policy**: The policy was released in 2013 which frames the vision and strategic way to shield the domestic cyberspace.
- **National Cyber Security Coordination Centre (NCCC)**: Made operational in August 2017 and its responsibility to make instantaneous risk calculation and generate situational awareness of probable cyber risks to the nation.
- **National Critical Information Infrastructure Protection Centre (NCIIPC)**: It is a national nodal agency, created under section 70A, for critical information infrastructure protection and its objective to protect critical information infrastructure (CII) from cyberterrorism, cyberwarfare and other threats.
- **Cyber Swachhta Kendra**: Cyber Swachhta Kendra, launched in 2017, offers a platform for users to examine and clean their systems of various viruses, bots/malware, Trojans, etc. [17].
- **International collaboration**: India has done nine bi-lateral agreements with developed countries such as the US, Singapore and Japan to promote research and information sharing on cyber security to combat advanced threats and to secure its cyberspace [18].
- **Sectoral and state CERTs**: Sectoral CERTs has been launched by the Government beginning with critical sectors such as power and finance. Further, state-level CERTs are likely to be formed [17].
- **Security testing**: There are plans to set up 10 further Standardisation, Testing and Quality Certification (STQC) testing facilities in India to evaluate and certify IT goods.

4. STEPS TO ENHANCE ICS SECURITY

It is the need of hour for organisations to implement rules and procedure starting from design, procurement, placement and operation of the ICS systems to combat cyber security. Sate bodies and regulators to identify the necessity for security of the sector and to setup nodal agency to protect Critical Information Infrastructure (CII) from cyberterrorism, cyberwarfare and other threats. Sector requires aid in terms of awareness and expert training, and guiding principle. Basic recommendations on the basis of survey conducted by KPMG [15] may be summarised as below:

- Availability of cyber security comprehensive policy with defined responsibilities.
- To impart required trainings to experts who are responsible to identify and prevent targeted attacks in the sector.
- Adhere to guidelines issued periodically by sectoral and national CERT to take precautionary measures and also report the attacks occurred.
- There should be collaborative effort of Technology and service provided in combating the risk completely.
- Periodic audit to be done to test readiness of cyber security by internal and external auditors.
- Risks reporting should be a part of formal reporting of risks and incidents.

4.1 Adapting Standards

Various standards have been developed by various government organizations, non-profit organisations and countries to deal with ICS threats. Some of the standards are nation specific and some of applicable universally [19]. These standards are the guidelines for organisations that use ICS machineries to develop 'defence-in-depth' strategies. Three main factors of these standards are Process, Technology and People [19]. Security of the system is ensured by all of three.

4.2 Applying Defence in Depth Tactics

A designed structure including People, Process and Technology has to be put in place to improve security through the organization, and also to conform to international standards and guidelines such as NCIIPC, NIST etc. [19]. Designing network similar to the reference implementation shown in Figure 5 will improve cyber security in better way. The research is on its great pace to standardise bench marks and tools for developed or are being developed infrastructure and control to make them secure. Lots of work needs to be done and various areas have yet to be entirely explored.

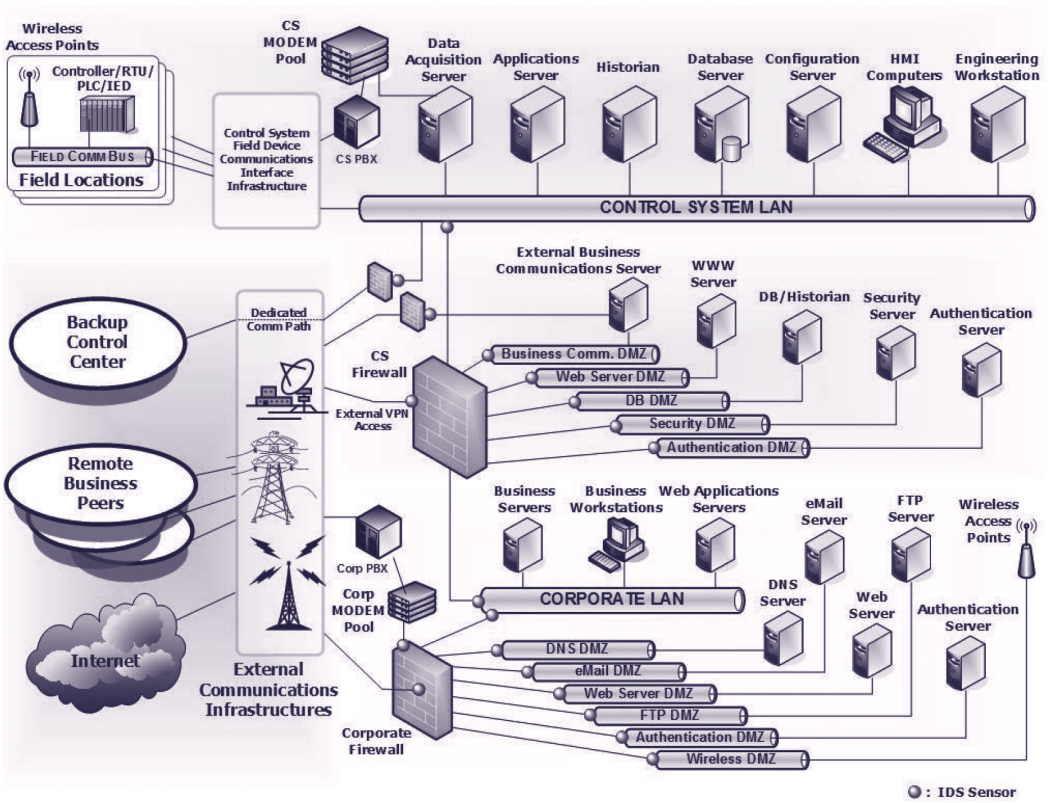

Fig 5. Architecture of control domain with use of 'defence-in-depth' strategies. [3]

5. CONCLUSION

Cyber-attacks can bring fiscal deficits, derail any nation from its estimated growth curve and fade relations with our neighbours, creating a situation of anarchism. To enjoy the benefits of technology, it is very much important for a developing digital economy like India to stress on cyber security and form a cyber-resilient atmosphere to protect from cyber-attacks. Being the Energy and Natural Resources (ENR) Sector as main sector for nation, any disruption will impact the economy as well as safety and security of the public employed in the sector and citizens in the neighbourhood of the installation. Universally the sector has seen major attacks on ICS systems which have affected facilities and societies. It

is good that India has not seen major attacks which is not by strategy but by coincidence as the sector is not equipped for targeted attacks as seen from various surveys. From various surveys conducted on threats to ICS it's obvious that attackers are discovering new methods to acquire access of systems by taking advantage of weaknesses that present from long time. Review of the ICS has revealed various security weaknesses which can, and are, being misrepresented regularly. The most noticeable fear is legacy ICS with no safety tools in place interfaced to the cyber world. This is an unsafe arrangement of old and new control system arrangements which can effortlessly be accessed by a reasonably computer knowhow hacker. It is encouraging from various surveys that businesses have noticed the risks and started working on it, which is attaining various level of maturity across business segments in the Sector. The concern is multifaceted and no particular stakeholder has ability to resolve all issues be it technology and service providers, industry, government and regulators as huge number of equipment exists which were not planned and installed with connected domain and cyber-attacks at design phase. CERT-In and NCIIPC circulates alerts and special reports related to critical infrastructure security and offers stage for different establishments to exchange knowledge and experiences in situation of cyber security lapses. This greatly aids in providing valued and in time feedbacks and supports them to proactively prepare to ease the threat.

REFERENCES

[1] G. Williamson, "OT, ICS, SCADA – What's the difference?", Kuppinger Cole, July 07, 2015. [Online]. Available: https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference

[2] T. Yardley, "SCADA: issues, vulnerabilities, and future directions", Vol. 33, No. 6

[3] D. Kuipers, M. Fabro, "Control Systems Cyber Security: Defense in Depth Strategies", May 2006, INL/EXT-06-11478.

[4] As India digitises, cyber crime is becoming an increasingly tangible threat, Consultancy.in, June 4, 2018. [Online]. Available: https://www.consultancy.in/news/1081/as-india-digitises-cybercrime-is-becoming-an-increasingly-tangible-threat

[5] R. Mahajan, "Risk Survey 2018 Transforming Risks into Opportunities", Deloitte, India, 2018. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-risk-RiskSurvey2018-noexp.pdf

[6] "Industrial control system (ICS) security", Pwc, India. [Online]. Available: https://www.pwc.in/consulting/cyber-security/industrial-control-systems/pwc-pov.html

[7] C. Kumar, Ransomware attack hits at least 100 systems in India, Times of India, 2017. [Online]. Available:https://timesofindia.indiatimes.com/india/ransomware-attack-hits-at-least-100-systems-in-india/articleshow/58663696.cms

[8] K. Stouffer, J. Falco, K. Scarfone, "Guide to Industrial Control Systems (ICS) Security", NIST SP 800-82, 2011. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

[9] J. Weiss, "Protecting Industrial Control Systems from Electronic Threats", Momentum Press, ISBN: 1606501976 9781606501979, 2010.

[10] D. Maynor, R. Graham, SCADA Security and Terrorism: We're Not Crying Wolf, 2006. [Online]. Available: http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf

[11] N. Cai, J. Wang, X. Yu, "SCADA system security: Complexity, history and new developments", 6th IEEE International Conference on Industrial Informatics, INDIN 2008, pp. 569–574, 2008.

[12] J.A. Falco, S. Hurd, D. Teumim, "Using Host-based Anti-virus Software on Industrial Control Systems: Integration Guidance and a Test Methodology for Assessing Performance Impacts", NISTSP 1058, 2006. [Online]. Available: http://www.uscert.gov/control_systems/practices/pcsf/groups/d/1177076007-nist_sp1058.pdf

[13] Dept. of Homeland Security, Recommended Practice: Improving Industrial Control Systems Cyber security with Defense-In-Depth Strategies, Control Systems Security Program, National Cyber Security Division, October 2009. [Online]. Available: http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf

[14] W. Schwab, "The State of Industrial Cyber security 2018", Kaspersky labs, White Paper, June 2018. [Online]. Available: https://ics.kaspersky.com/media/2018-Kaspersky-ICS-Whitepaper.pdf

[15] "Cyber security survey - Operational technology Energy and Natural Resources", KPMG, India, June 2018. [Online]. Available: https://assets.kpmg/content/dam/kpmg/in/pdf/2018/08/cyber security-energy-natural-resources-operationa.pdf

[16] Global Cyber security Index, International Telecommunication Union, 2017. [Online]. Available: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf. [Accessed: 23- Aug- 2017].

[17] Ministry of Electronics and Information Technology (MeitY) launches Cyber Swachhta Kendra - Botnet Cleaning and Malware Analysis Centre, 2017 [Online]. Available: http://pib.nic.in/newsite/printrelease.aspx?relid=158620

[18] Mapping of India's cyber security-related bilateral

agreements, The Center for Internet & Society, 2016. [Online]. Available: https://cis-india.org/internet-governance/blog/india-cyber-security-bilateral-agreements-map-dec-2016. [Accessed on 23- Aug-2017].

[19] "Industrial control system (ICS) security", Archives of PwC, Vol.7136, August 2016. [Online]. Available:https://www.pwc.in/assets/pdfs/consulting/cyber-security/industrial-production/industrial-controls-system-ics-security.pdf

[20] R. Sharma, "Study of Latest Emerging Trends on Cyber Security and its challenges to Society", International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012

AUTHORS

Mahesh Singh, PhD Student, School of Management, G. D. Goenka University, Gurgaon – 122 103, Haryana
Email: maheshsingh2775@gmail.com

Dr. Kishore Kumar Morya, Associate Professor, School of Management, G. D. Goenka University, Gurgaon – 122 103, Haryana