Cyber Security: Way Forward

SCOPE in association with DSCI conducts workshop on "Approaching Cyber Security Challenges in CII Sector"

Dr. Sanjay Panda, former Chief Secretary, Govt. of Tripura & former Secretary to Govt. of India, Ms. Neeta Verma, DG, NIC, Mr. Sanjay Bahl, DG, CERT-IN, MEITY, Mr. Rakesh Maheshwari, Scientist G & Group Coordinator, MEITY, Mr. Vinayak Godse, Vice President, DSCI and Mr. P.K. Sinha , SCOPE during the inaugural session of the workshop.

Public Sector Enterprises (PSEs) are the critical stakeholders in driving the national economy. Their astute presence in the lifeline sectors of the nation i.e. Oil & Gas, Energy, Infrastructure, Services, Defence etc. is the proof of its acute significance. As the world is witnessing the fourth Industrial Revolution in the form of digitalization, organizations across the globe are digitalizing their operations and functions. The flow of information is tremendous and hence, the dependability. Public Sectors are not aloof from it and are adopting the technology with zeal and need. Whether it is adapting cloud or moving information to cloud, PSEs have been moving with market. Being an economic power in itself, its digital security, therefore, is of paramount national importance. The threat landscape keeps on changing and is now different than before. Therefore, it is important that we protect our Critical Information Infrastructure (CII) from hostile intruders/attackers and enable readiness to meet any such challenges.

Standing Conference of Public Enterprises (SCOPE), therefore, in association with Data Security Council of India (DSCI), a body set up by NASSCOM, organized a One-day workshop on 'Approaching Cyber Security Challenges in CII Sector' on 12th October 2018 at SCOPE Convention Center, New Delhi. Dr. Sanjay Panda, former Chief Secretary, Govt. of Tripura & former Secretary to Govt. of India inaugurated the workshop in the presence of Ms. Neeta Verma, DG, NIC, Mr. Sanjay Bahl, DG, CERT-IN, Ministry of Electronics & Information Technology (MEITY), Mr. Rakesh Maheshwari, Scientist G & Group Coordinator, MEITY, GOI, Mr. Vinayak Godse, Vice President, DSCI and Mr. P.K. Sinha of SCOPE.

Welcoming the participants and dignitaries in his introductory speech, Mr. P.K. Sinha of SCOPE said that Cyber Security is subject of global challenges and for that reason many of developing countries have taken up cyber security as national agenda and are devising national policies on this emerging issue. He further added that, PSE being strategic partner in the socio-economic development of the nation makes them a key stakeholder and with that their cyber security is of national importance. With this in view and profound support from Knowledge Partner, DSCI, this theme was selected for Workshop.

Giving the program perspective, Mr. Godse said that operating environment is getting integrated to IT. If we look at a particular threat, he said, one particular compromise could lead to not only the organization but the

(From L-R): Dr. Sanjay Panda, former Chief Secretary, Govt. of Tripura & former Secretary, GoI, Mr. Sanjay Bahl, DG, CERT-IN, MEITY and Ms. Neeta Verma, DG, NIC addressing the workshop.

whole society and the nation. He further added that Critical Sector are critical to national security and although there is lot awakening in PSEs, this debate has to filter down to minute levels. He said that intense debate on cyber-attacks is need of the hour.

In his address, Mr. Maheshwari, Group Coordinator, MEITY said that role of people process technology is paramount. He opined that security has to be seen as whole life cycle and not at a certain point. Talking about the rapid growth of mobile phones and access to internet, Mr. Maheshwari said that more and more people have access to internet resulting in growing usage of cloud, social media which from personal experience makes work easier but from security purpose creates more complexities. He added that Cyber Resilience is the name of the day. Talking about the IT Act and its satisfying provisions to secure cyber frontier, he added that a major point missing in the IT Act is about the declaration of critical infrastructure within a organization. He apprised the gathering that Ministry is soon coming with Data Protection Bill which would enhance the cyber security.

DG, NIC, Ms. Verma in her keynote address discussed in detail about the changing threat landscape, complexity of attacks viz. state sponsored, organized criminal activities, personal gain etc. DG, NIC added that Digital India Program has resulted in Data revolution and as a result, many vectors have resulted into driving cyber security as well as attack. PSEs, she said, play significant role in nation with their presence in every key sector like defense, banking, telecommunication power etc. She further added that PSEs have adopted digitalization in form of ERP, HR Management system and are also moving their IT system to cloud based. She also discussed challenges that PSEs face in terms of scale, vast Geographic Boundaries, Interconnectedness that could lead to cascading effects, Integration with IT Networks, Coordination amongst PSEs etc. She advised that there should be a comprehensive approach for cyber security and it is by the holistic approach we can have a secure cyber space. Talking about the need to generate awareness and skill building in PSEs, she added that multilayer security, use of analytics and Artificial Intelligence (AI) could provide a secure cyber space. She also highlighted key considerations for CII Security like strong cyber security team, policy regulations and best practices, regular audit, emergency response system, cross sector co-ordination, cyber threat intelligence, and robust infrastructure.

DG, CERT-IN, MEITY, Dr Bahl in his keynote address emphasized the need to be aware of cyber threats to know who is doing the scanning and when they are doing it what are they looking for. Mr. Bahl pointed out that there is lack of awareness about cyber security threats amongst users, lack of proper response plane and lack of skill-sets. He also added that unclear roles and responsibilities in time of attack, lack of forensic readiness, organization not reporting incidents have made the matter even more complex. He posed seven questions before the participants to ensure cyber security in their respective organizations-

- Do you have people to manage your industrial control systems?
- Do you know what you have installed in the field?
- Do you have true cyber security control system in place?
- Can you trust the output from your devices?
- Do you have right documentation for your system?
- Do you fully understand

network access issue?

- Are your incident response and capabilities in place?

Chief Guest, Dr. Sanjay K. Panda, IAS while delivering the inaugural address said that PSEs were set up as engineer of growth and even today, they are playing an important role in socio-economic development. Former Chief Secretary, Govt. of Tripura & former Secretary to Govt. of India further opined that we are witnessing fourth industrial revolution in form of AI and big data and therefore, we have to keep adapting new technologies as technology is changing rapidly. While discussing his experience as Chief Vigilance Officer in SAIL, he advised the participants to be vigilant as the process needs to be preventive. He also said that Central organization should constantly guide executives from PSEs and PSEs in turn should adapt customer friendly technology as the 90% of the workforce are not as tech savvy as IT Experts.

Vote of thanks for the Inaugural Session was proposed by Mr. Sinha expressing sincere gratitude to all Dignitaries on Dias, Ministry of Electronics & IT, GOI, CEOs of PSEs for sending delegates, Invitees and Eminent Speakers.

Post inaugural session, a panel discussion was conducted on "Future of Control Engineering: What it means to security of SCADA/ICS. Mr. Ramesh Kumar, Chief Manager, GAIL-TEL, Mr. Jayant Gupta, CGM IS, HPCL and Mr. Dharmendra Kumar, CISO, Tata Power Delhi Distribution were the panelists while Mr. Vinayak Godse, VP, DSCI moderated the session. The panelists highlighted the digital infrastructure in their respective organizations. They were of the opinion that Digitization Index in organizations are needed to identify processes IT has to do. They also said they are also using Big Data to predict the feeder problem with 86% success rate. Much of the controlled system, they said have been integrated and even more integration points are demanded to which they cannot say no to which has resulted into a lot of complexities in order to secure them. They also opined that we need to look at the system to identify nodal points, look at devices, channels and need to control all of them at the same time. Panelists also gave examples of how they are using technology to enhance safety. For example in GAIL, Quality of the Gas gets affected in presence of sulfur and humidity. Therefore, they get data of the source gas and if it goes into alarm level, the supply gets closed automatically. While they were of the opinion that Original Equipment Manufacturer (OEM) should not be given access to remote connectivity, some OEMs have come up with their own solution. The panel also opined that the best practices should be compiled and can be help of us with cyber security. Expressing their concern over the remote connectivity, they said that they are vendor driven and although technologically it is possible to control it, but security wise it is an issue of concern. They also advised the gathering to take Vulnerability Assessment of Operating System.

The session was followed by a discourse on "Myths & Realities of OT/IIOT" by Mr. Mayank Lau, Principal Consultant, DSCI. Mr. Lau gave an overview of the Industry 4.0 where engineers troubleshoot the problem from remote site using enhance technology like 3-d printing. He also gave examples of Cyber Attacks namely, Iran, 2010- somebody studied

Iranian nuclear plant for two years- and bugged it with Stuxnet virus. Stuxnet is a malicious computer worm, first uncovered in 2010. Thought to have been in development since at least 2005, Stuxnet targets SCADA systems and is believed to be responsible for causing substantial damage to Iran's nuclear program. He also gave an example of a disgruntled employee who in Australia conducted a series of electronic attacks on the Maroochy Shire sewage control system after a job application he had made was rejected by the area's Council. At the time he was employed by the company that had installed the system.

Mr. Lau added that industries need to adopt Threat hunting i.e. scan the adversaries and don't limit your-self to equipment. He briefly highlighted various Security Challenges viz.

- Targeted by advanced persistent threats
- Identification of CII
- Mitigating risks in the cloud environment
- Assessment on cyber threat preparedness
- Lack of detailed guidelines and SOPs
- Real time monitoring and incident mechanisms
- Mitigating risks of remote maintenance
- Data classification
- Protecting SCADA devices

(From L-R) Mr. Rakesh Maheshwari, Scientist G & Group Coordinator, MEITY, Mr. P. K. Sinha , SCOPE and Mr. Vinayak Godse, Vice President, DSCI addressing the workshop.

Coming onto the topic, he explained myths and realities concerned to cyber security. He divided his presentation into three parts namely, Myth, Reality & Best Practice. Few examples given by him are as ollowing:

Myth	Reality	Best Practice
IT & OT can't have single CS Strategy	Look for similarities from design & risk	Cross Trainings
OT Risks are same as IT risks	Operations & Business Disruption	Integrated Risk & practice
Cloud AI CS Solution not of IIOT	Rue to an extent	• Avoid mission critical systems • To leverage data sets of other organizations
IT, IIoT handled by single team	Multiple teams can exist	Staged approach to build CS team
Air gap is dead	Still deployed in asset centric organizations	Rigid access Controls
Apply IT CS design and management	OT system are real time event driven	• Rigid segmentation policies for OT systems • Start from Industry standards • Assess OT Risks initially • Identify specific security controls

He further added that we have this problem of only analyzing security data or log and there is a need to leverage data and integrate IT & OT to deliver IT/OT business benefits.

The session was followed by a panel discussion on "Critical Sector Attack" where the panelists Mr. P K Agarwal, CISO, POSCO, Mr. Manoj Kumar Jha, CIO & Head of IT BEML, Mr. Anil Joshi, GM, Corporate Digital Transformation, BHEL and Mr. Altaf Halde, Global Business Head, Network Intelligence. The panel was of the opinion that over the years SCADA system has developed. They also said that there is no repository of events of cyber attacks and in absence of such kind of exposure in our country per se exposes organizations to the threat issues. They advised the participants that we need to act sooner than later as the systems can't be kept in isolation for long. They advised that organizations should do aggressive auditing and have proper log of events which is not very intensive. The panel said that there is nothing such as absolute security, we just have to monitor the enter point from OT to IT.

Awareness, they opined, is the biggest challenge organizations face. To strengthen the cyber security, panel was of the opinion that there is a need to make SCADA system more strong, ensure Supply Chain Security, adapt cloud tech. They said that end user level awareness and sensitizing them is of utmost importance. Speaking about the threat, they said it has to be decimated to the entire spectrum.

The panel also threw light on indigenization of technology. They said organizations use high end technologies that are basically from European companies. This results in solutions coming at a huge cost. They said that industry should invest in R&D to develop indigenous technologies to deal with threat.

Speaking on the Reporting

Team
- **OT security response is a big problem**
- **Understanding of OT Security**
- **Certification training for OT, Leadership development**
- **Formal Policy**
- **Should be within the nation**
- **Skill-sets**
- **Lack of Training Institutes**

App Management Systems
- **Mobile**
- **Sensitive Data might get leaked**
- **Security Authorization**
- **Not looking into security aspect while designing App**

Data Exchanges
- **Vulnerable to State sponsored attack**
- **Should be located within the country**

System in India, the panel said that Incident reporting is difficult in the Indian Environment and there should be transparency in reporting.

Highlighting the Operational Technology (OT) within organizations, they said skill sets need to be developed for OT resource also and organizations should have a policy for OT. They also requested the Indian organizations to motivate top talent to avoid brain drain to top tech companies of the world. Speaking on the training of employees, they said a User Awareness Matrix is also needed to see the efficacy of such training/awareness programs. The panel also pushed for OT certification which currently is missing in India. Later, Ravi Hirolikar, VP and Global Head of Information & Cyber Security, Data Privacy, Business Continuity- EXL presented his views on „From SOC to Cyber Defense Centre: A journey. He apprised the gathering by giving examples of cyber-attacks and said that we need to follow Microsoft's approach which they call- Assume the breach approach. Mr. Hirolikar further said that attackers are ahead of defenders and highly equipped. Ability to detect successful intrusion, he said, takes hours, days, months or years. Talking about System on a chip (SOC) he said, SOC in recent pasts or traditional SOC, revolved around logs and alerts, focused on monitoring only and had an isolated approach to incident management. It did not focus on Advanced & early detection. He said the time is ripe to move from SOC to Cyber Defense Centre (CDC). Giving a comparative analysis, Mr. Hirolikar said that CDC offers, well-orchestrated incident management, Rapid containment Prompt and Apt analysis of malware & containment. He said that cyber security is all about how early you detect threat and how quickly you respond. He also highlighted factors for success namely, contextual Asset Inventory, Policies & Procedures, Adequate Preventive Controls, Optimal Logging Baseline, Continual Assessment of detection & response capabilities.

The finals session of the day was an interactive module on Critical Thinking in Critical Sector Security conducted by Mr. Vinayak Godse, VP, DSCI. Mr. Godse gave various parameters to the participants like- Vulnerability Management,

Integration & Challenges, External Media, Data Exchanges, security testing etc. The participants were then asked to respond to these parameters on how they are using it, what steps need to be taken, to identify challenges and what they think about it. Few suggestions that came from the participants are given in the chart below.

The workshop was participated by a large number of executives from PSEs. Mr. P. K. Sinha of SCOPE thanked the Participants, Speakers, SCOPE & DSCI Organizing Team Members and also assured the gathering of conducting similar programs to strengthen the cyber security of CII Sector.