



Workshop on Approaching Cyber Security Challenges in CII Sector

12th October 2018

10:00 AM- 05:30 PM

SCOPE Convention Centre

Lodhi Road, New Delhi



**DATA
PROTECTION**



**NETWORK
SECURITY**

**INFORMATION
PRIVACY**

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.

CII are those interconnected information systems and networks on which nation's economy, security, health and functioning depends. PSEs being the backbone of the nation have also come under the radar of such cyber security threat and if not dealt prominently it will possess a serious & devastating threat to critical infrastructure. Potential adversaries have invested significantly in cyber space as it provides them with a viable, plausibly deniable capability to target the Critical Information Infrastructure and damage India's interests.

Given the apparent risk to the critical infrastructure, security is paramount and requires significant investment of efforts to secure it holistically. The risks and threats need to be adequately quantified to develop a robust security posture which can be effectively deployed in Industry Control Systems. Traditionally, CII were operated as separated networks disconnected to public communication infrastructures, but as businesses have turned to exploit the services and data provided by the Internet, such isolation that protected these systems is making it vulnerable to the cyber-attacks. Real time monitoring, peer to peer communications, multiple sessions, concurrency, maintenance and redundancy have enhanced the services provided for consumers and operators. The interconnectedness is further growing with the implementation of smart grids and execution of the Internet of Things (IoT). The traditional isolated systems have become exposed to a range of threats. SME supply should be available to understand the deployed components such as Programmable Logic Controllers (PLC) or similar Intelligent Electronic Devices (IED), Remote Terminal Units (RTU) and input/output (I/O) devices that are used to manage electromechanical equipment in either local or distributed environments.

State and non-state actors threaten disruptive and destructive attacks against India and conduct cyber-enabled theft of intellectual property to undercut the India technological and defence advantage. We are vulnerable in cyberspace, and the scale of the cyber threat requires urgent action by leaders of PSEs. A resilient cyber security program is utmost required so that cybercriminals cannot have an effect on the way in which our economy and nation operate, those that the critical infrastructure sectors have worked so hard to build over many years.

ABOUT SCOPE

Standing Conference of Public Enterprises (SCOPE) is an apex professional organization representing the central public enterprises. It also has some state enterprises, banks and other institutions as its members. SCOPE's objective is to promote excellence in organizations where Government investment is involved. Its vision is to enable member enterprises to be globally competitive in a market-driven environment.

ABOUT DSCI

Data Security Council of India (DSCI) is a not-for-profit, industry body on data protection in India, setup by NASSCOM®, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. To further its objectives, DSCI engages with governments and their agencies, regulators, industry sectors, industry associations and think tanks for policy advocacy, thought leadership, capacity building and outreach activities.

In this table top paper based exercise, organisation leaders will have to identify cyber threats and create response plan to the cyber attacks and threats based on real-world scenarios identified during the exercise. After the paper based immersive workshop, senior executives will have a good idea of how prepared their organization is to defend itself against a surprise security breach.

Key Learnings

- Threat landscape for critical sector organizations
- Challenge of CII Sectors : Sectoral Insights
- Building Cyber Security Strategy
- Enterprise liabilities due to vulnerabilities
- Compliance and Security Interconnectedness
- Methods to Prioritize Prevention
- Elevating Cyber Security Risk to Enterprise Risks
- Reciprocity Strategy During Attack Emergency
- Changing Security Paradigm

Participation

- Decision Makers
- Middle & Senior Level Management
- IT/Technical Experts

Faculty

- Eminent IT & Cyber Security Professionals/Experts

Workshop Facilitators

Mr. P.K. Sinha
Head (HR& CC), SCOPE
Mob: 9810308456
Email: pramodks.scope@gmail.com,
pramodks@scope-online.in
Website: www.scopeonline.in

Mr. Amit Verma
Deputy Director, DSCI,
Mob: 9810748822
Email: amit.verma@dsci.in
Website: www.dsci.in

Programme Details

Venue: SCOPE Convention Center, SCOPE Complex, 7 Lodhi Road, New Delhi - 110003.

Dates: 12th October, 2018

Registration: 09:00 a.m. to 10:00a.m on 12th October, 2018

For any clarification, you may also call Sunil Sharma | Marketing Manager,

DSCI P: +91-120-4990253 | M: +91-9910820644 and

Mr Rishabh Kumar / Ms. Garima Agarwal, Executives of SCOPE

P: +91 11 24369740, 24361757

Course Fee

Rs. 5,000/- + GST (18%) per participant

Course fee can be paid by cheque/DD favouring "Standing Conference of Public Enterprises".

Payment can also be made through ECS mode as per details below:

Dena Bank, SCOPE Complex Branch

Lodhi Road, New Delhi- 110003

Saving Bank A/c No. 105010001856- MICR Code 110018021

IFSC/RTGS Code BKDN 0711050 • GSTIN07AAPFS7390N1Z7

Delegate Registration

Nominations may please be sent to:

Workshop Co-ordinator

Mr. A. Zaman, Senior Manager (HR)

Ph : 011-24361747, Mob : 9868502306

Email: programs.scope@gmail.com, programs@scope-online.in

www.scopeonline.in