INTERNATIONAL CENTRE FOR
CHEMICAL SAFETY AND SECURITY

BUILDING AWARENESS ABOUT CYBER THREATS AND INCREASING RELIABILTY AGAINST CYBERATTACS IN THE COMPANY

TRAINING OFFER ADDRESSED TO ALL WHO SUPERVISE, MANAGE AND OPERATE RELIABILITY AND CYBER-SECURITY IN A COMPANY

BASIC TRAINING OFFER

CONTACT
Mr. Adam Paturej
ICCSS Cybersecurity and Reliability Director
International Centre for Chemical Safety (ICCSS)
ul. Leszno 8/1; 01-192 Warsaw
Tel: +48 22 436 20 44
e-mail: a.paturej@iccss.eu
www.iccsss.eu

WHY ICCSS?

ICCSS – international leader in the development of Cybersecurity-Resilience against cyber attacks and Reliability:

- The ICCSS concentrates on raising awareness of cyber threats: Gaining knowledge concerning various types of attacks is the first step to secure the enterprise
- The ICCSS develops cybersecurity culture and promotes best practices to reduce vulnerability on cyber threats
- The ICCSS developed and implements a unique training programs
- The ICCSS develops professional competences in the topic of Cybersecurity and Operational technologies (OT)
- The ICCSS implements intelligent technical solutions by using digital data system instead of paper

ICCSS promotes digital integrity of systems which provides safety, security, reliability, integrated Risk Based Management:

- Gaining and sharing current trends in the development and implementation of the best cybersecurity policy practices
- Establishing a cybersecurity platform as a part of the roadmap for the industry cooperation, development, and implementation of security programs
- Small and medium sized enterprises will receive an access to free cybersecurity programs and reliabilityimprovement - tailered approach to cybersecurity

By managing reliability – element of cybersecurity and improving immunity to the cyber-attacks, ICCSS supports:

- Digital data
- Upgrading of processes and business procedures
- Conducting inspections on the basis of Risk Based Inspection model
- Cooperation with supervisory authorities
- Extending asset equipment life cycle
- Reducing cost.

OUR ASSETS

ICCSS benefits from US partners on standards and best practices:

- Cooperation with US Department of Homeland Security
- Use of US security solutions for the chemical infrastructure in US
- CSET 7.0 – vulnerability assessment
- CSAT 2.0 – Security analysis for the chemical industry
- Database for procedures and the best policy practices
- Supporting enterprises in cyber-danger immunity
- Development and conduct of unique training program on increasing resilience against cyber threats and cybersecurity culture
- Digital integration of systems which provides safety, security, reliability, and risk-based management

Software based solutions for management of chemicals:

A unique system collects digital versions of all data and documentation related to the safety of the plant and make it available to eligible and responsible persons in the plant as well as from the external authorities / organizations if needed and allowed, e.g. Fire Brigade, Office of Technical Inspection, Inspectorate for Environmental Protection. In addition to data collection, the system can be also used for monitoring and supervising tasks that are related to Accident Prevention Program and Safety Management System, e.g. maintenance activities, monitoring and diagnostic procedures, training of employees. The software is in line with the Seveso III Directive of the EU.

Access to international partners and their capacities:

Since its foundation in 2012, ICCSS has been active in promoting global initiatives in the area of chemical safety and security through organization of conferences. This allowed us to develop an extensive network of partners that share the common vision of the safer environment.

Management system solutions:

Apart from the chemical-related issues, we show a strong focus on effective management system. We offer help in implementing ISO 27001:2005 standard, which puts information security under strict management order. Moreover, together with AGH University of Technology, we are developing a unique OKIT methodology - a structured method for the development of security management system for an effective protection of information assets in industry and systems that are used to store, process and transmit sensitive information.

ICCSSS TRAINING OFFER

BUILDING AWARENESS ABOUT CYBER THREATS AND INCREASING RELIABILTY AGAINST CYBERATTACS IN THE COMPANY

TRAINING OFFER ADDRESSED TO ALL WHO SUPERVISE, MANAGE AND OPERATE RELIABILITY AND CYBER-SECURITY IN A COMPANY

Each day we hear news about hackers hijacking bank accounts, or about loss of huge of data, what reminds of the importance of IT (Information Technology) systems. Cybersecurity for industrial processes (OT – Operational Technology) is equally important. The effects of a cyber attack on OT systems at industrial facility can be catastrophic for the company's operations, property, health and life of employees and the environment. Industry 4.0 will bring ever-wider connection of industrial machines and equipment via Internet what will increase cyber risks and threats.

Ensuring adequate reliability of control systems and thus the OT cybersecurity in an enterprise is a condition sine qua non for safe handling of industrial processes and business operations.

We offer training which promotes cyber security as a core element of the broadly, holistically understood "security and protection" of the enterprise. The training was developed based on cooperation and studying the experience of the US Department of Homeland Security.

The training concentrates on practical aspects of increasing industry resilience against cyber threats by introducing cyber security culture and raising awareness and Staff preparedness, sharing best practices, and providing ready solutions for verifying resilience against cyber threats, for decision-makers and technical Staff, as a process of continued improvement. Process approach means, among others constant monitoring and reacting to cyber incidents, documenting events and quick undertaking of improvement actions. The great advantage of the training is that the proposed approach does not interfere in the IT system, does not collect data and does not conduct any analysis and audit. The training enables company Staff to conduct a cyber threat analysis and produce a report on the greatest risks and areas for improvement of cyber safety which could be most quickly repaired (so-called QuickFixes). Training will enable to conduct vulnerability and resilience tests by the company representatives of the company, what will ensure that results remain in the enterprise.

SCOPE OF TRAINING 1- day, initial training on building awareness and resilience against cyber attacks. A database of questions will be demonstrated to allow a comprehensive analysis of cyber security issues in a company according to the principle of Deep Protection of Enterprises (Defense in Depth). The questions are based on American NIST and NERC standards as well as industry standards widely used in the USA, as well as being extended to ISO and ISA standards used in Europe. Printed training materials will be provided, which contain, among others, questions comprised of cyber-resilience analysis, and tools available in the US to test cyber-resistance.

INTERNATIONAL CENTRE FOR CHEMICAL SAFETY AND SECURITY

Working together to enhance chemical safety and security

ul. Leszno 8/1
01-192 Warszawa
Polska
(phone – office) +48 22 436 20 44

www.iccss.eu ; info@iccss.eu