Building resiliance against cyber attacks - developing cybersecurity and reliability

ICCSS organization and development of the cybersecurity training program

Our approach

cybersecurity-resiliance-reliability

- Since its establishment ICCSS has focused on the devlopment of broad access to safety and security and the devlopment of training methodologies.
- ICCSS is a leader of **Train The Trainers** approach, to share best practices and apply the knowledge in practice;
- We have access to worlwdie partners from governments, industry, academia;
- We develop training curricula and facilitate companies to implement the solutions on their own.

- ICCSS is not a consulting company:
  - given our network structure it is difficult for us to provide consulting services on a regular basis.
  - We therefore welcome partnerships with companies who are able to further lead the topic in case of specific client's needs.
  - Our training approach very well establishes **a need/demand for technology solutions** which by nature ICCSS is not able to satisfy.

ICCSS approach to cybersecurity

- Our main strength has always been **operationalization** and **operationalization** of the exsiting best practices and capacity building;

- We have taken a similar approach in industrial cybersecurity:
  - Primary importance given to management policies, establishing teams, and development of appropriate procedures, based on exisiting solutions. Technology and software come afterwards.
  - OT Cybersecurity discussion has to start from the Board level and move to all copmany levels;

- Leading task is the development of a **company cyber security culture**

- Building a cybersecurity is **a whole organizational effort** with multiple stages – **whole-company cyber-security approach**.
  - ICCSS helps company build cross-functional teams and assists in **integrating cyber-security culture with the cyber-security technical solutions**.

ICCSS leadership in industrial cybersecurity worldwide

Building upon…

- our industrial contacts and trust we established among industry through various programs
- working level cooperation with Department of Homeland Security and in-depth knowledge of the standards and procedures available in the US
- growing rise of threats against industrial control systems and the fact that no one at that time in Poland had a consistent industrial cyber-protection system

The ICSS has developed a dedicated training program for ICS cybersecurity to fill this gap;

- There was a major awareness campaign conducted to promote industrial cyber-security since OT cybersecurity has either been neglected or at best treated in a similar fashion to IT security. After 2 years of active cooperation and campaigns within the industry, we started trainings with a **unique approach** – to increase resiiance against cyber attacks and develop cyber-security culture in company
- There are no direct competitors for OT cybersecurity training in Poland or similar approach. Training companies offer trainings to implement the exisitng technical solutions;
- ICCSS comes esarlier – we offer companies tools and experiece how to measure their resilience, develop internal capacity and to introduce whole-comapny and integrated approach to protect against cyber attscks.

Managing reliability – element of cybersecurity and improving immunity to the cyber-attacks

- 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
- Improving safety and security

ICCSS OFFER – help integrate cyber-security needs and culture with the cyber-security technical solutions in industry

- To train company Staff on cyber-security, with emphasis on sales teams to prepare them for dialogue with clients on developing background company knowledge and culture on industrial cybersecurity;
- To introduce cyber-security training and cyber-security culture at relevant companies – **to build a model approach**: 1) develop company cyber security culture; 2) verify resiliance against cyber threats; 3) introduce best practices, standards and ICS cyber software.

ICCSS Provider of training methodologies and expertise

- Providing training methodologies and expertise
  - Focus on procedures, management systems, risk management, security vulnerability assessments
  - ICCSS as the knowledge Centre and contact point for best practices in the chemical sector
  - Development of training curricula , tabletop and full scale exercises
- Member and leader of various consortia in EU projects and others.
- Organizer of symposia and conferences with training as a major issue
  - Our yearly event: Global Summit in Chemical Safety and Security (CHEMSS) (www.chemss2017.org),
- **Cybersecurity program** – developed since 2015 using our experiences and partners from other fields (especially US Department of Homeland Security and industry partners in Poland)

ICCSS initiatives on cybersecurity

- Program to develop insurance products for companies with Industrial Control Systems (ICS)
  - Part of the large consortium with PZU, Institute for Automation and Robotics, AGH University of Science and Technology, Kosciuszko Institute. We are the providers of training methodology and awarenesss campaign.
- Joint white paper for with Office for Technical Inspection, PZU, Warsaw Technology University, Kosciuszko Institute, for defending the ICS at the time of Industry 4.0
  - Presenting the values of industrial control systems and the need for their protection. Published during CYBERSEC forum – the largest venue for cybersecurity in Poland
- CHEMSS 2017 – Global Summit on Chemical Safety and Security
  - Organized by ICCSS, 2000 people attending, 50 countries
  - Consultations on reliability and cybersecurity of Industrial Control Systems
- International Conference on Cybersecurity and Reliability for Industry 4.0 (Warsaw, 30 August, 2018)
- Initiator at the G7 Global Partnership the issues of cybersecurity for chemical and Energy carriers industries

ICCSS and industry cybersecurity

- Cybersecurity of operational technology is the major topic of CHEMSS2016, CHEMSS2017 and programs concerning chemical safety and security
- the pioneer of developing Cybersecurity culture, white book, and roadmap in the chemical industry and energy transmissions
- the pioneer of compiling a cybersecurity workbook to share good policy practices in the operational technology, reliability, and immunity to cyber-attacks
- the organizer and sponsor of annual conference of **Reliability and cybersecurity in Industry 4.0** (in cooperation with Warsaw University of Technology)
- the initiator of integrated security audits in Information Technology and Operational Technology
- the author of training program for developing immunity to cyber danger and security of cybersecurity in the industry

ICCSS Cybersecurity activities in Poland

- Trainings conducted:
  - LOTOS Group (2nd largest petrochemical group in Poland) - training a team of 15 people (Management Board, OT and IT Director, Security Director, network administrators)
  - Series of introductory trainings organized by ICCSS in partnership with PZU (largest Polish insurance group) to the following audience:
    - Enea, Tauron (distributors of energy) PGE (largest energy producer in Poland, PKP Cargo (railway logistics) , PGNiG (largest gas producer and distributor in Poland), Orlen (petrochemical), Azoty group, Anwil (chemical plants)
- Conference and workshops
  - Experts from ICCSS regular speakers at conferences.
  - Part of the content generating teams for the below conferences:
    - CYBERSEC (https://cybersecforum.eu/en)
    - Cybersecurity of Industrial Control System organized by Nowa Energia- the most important venue for ICS related topics in Poland.
- All of the above helped us to develop a solid customer base

ICCSS cybersecurity Goals for 2020

- Develop market for OT cybersecurity by introducing professional competences
- Introduce road map for OT cybersecurity in chemical industy and Energy carriers;
- Conduct a series of awareness trainings and best practices exchanges within the program: ***OT cybersecurity under the roof of industry***;
- Extend OT cybersecurity to Small and medium Sized Companies, with emphasis on local providers of critical infrastructure services and core services
- Partner with a technology providers to integrate safety-security-reliability in OT cybersecurity in ICCSS programs

Lack of preparedness to cyber threats within international organisations dealing with chemicals

- The international organisations do not develop measures to protect industry neither the supply chain from cyber attacks
- Cyber security shall be one of the elements of the broadly, holistically understood "**the peaceful applications of chemistry" and industry development cooperation**

ICCSS approaches to cybersecurity at OPCW

- ICCSS promotes partnerships in strengthening cybersecurity in the chemical production and supply chain with National Authorities, chemical industry and Technical Secretariat
- ICCSS will share best solutions, based on its international contacts, partnerships and gathered experience.
- ICCSS focuses on sharing CYBERSECURITY CULTURE and development and conduct of **cybersecurity trainings**.

ICCSS cybersecurity offer for international organisations

- Provide, free of charge, training course methodology on awareness and raising resilience trainings on the chemical facility cyber protection
- Partner with National Authorities to conduct background courses on awareness and raising resilience trainings on the chemical facility cyber protection
- Provide, free of charge, methodology and concept of developing competence capacities in cybersecurity and resilience in industry
- To train international staff on cybersecurity and resilience in chemical industry

Working together to enhnace chemical safety and security

Contact

Adam Paturej (e-mail: a.paturej@iccss.eu)