Contribution ID: **543** Type: **Paper**

Computer Security Training and Exercises in the Nuclear Sector: Insights from a User-centered Requirements Gathering Process

Computer security is recognized an important aspect of nuclear security, as highlighted by Resolution GC(62)/RES/7 of the IAEA 62nd General Conference (2018), which encourages States to take effective measures against cyber-attacks. An important measure –highlighted in the Resolution –is the provisioning of computer security training courses. The nuclear sector, with support from agencies such as the IAEA, is responding to the need for training and exercises. As the sector's response matures, it is useful to understand and evaluate the current state-of-play, as perceived by the (potential) recipients of training. With this understanding, informed guidance about future strategic directions for training and exercises can be made, to ensure that initiatives provide the most benefit to participants and the sector.

The contribution of this paper is two-fold: first, we describe a campaign for gathering requirements for computer security awareness and training in the nuclear sector, which was conducted in the framework of the IAEA's CRP J02008 (Enhancing Computer Security Incident Analysis at Nuclear Facilities). In this context, we share a set of challenges and recommendations for implementing user- and stakeholder-centered thinking in the given multi-stakeholder setting. We critically reflect approaches to implement an iterative consultation process and to embed diverse user involvement tools into this process, such as audience participation and personalized electronic questionnaires.

The second contribution is a survey of the status of computer security awareness and training within the nuclear sector, as yielded by the requirements gathering process. Participants from thirteen countries across different roles and organization types (e.g., operator, regulator, policy maker, contract support) engaged in an electronic questionnaire and personal interviews that aimed at identifying the perceived computer security risks, the current state of computer security education within their organizations, as well as impediments to education and key improvement measures for increased awareness and protection.

The results of our research show that safety system operation ranked highest among seven different areas of risk, and that 'removable media and devices'was the most strongly perceived attack vector. Participants outlined the most important impediments to increasing computer security awareness and skills in their respective organizations –namely, a lack of management focus and support, a lack of priority or applicability, and insufficient personnel to conduct the training. According to the respondents, the human factor is considered in nuclear computer security programs of their organizations, but education is often regarded limited. The current focus of computer security training in many facilities is on building awareness and development of skills, and less targeted at regulatory compliance, process validation or skills re-enforcement, which reflects the emerging nature of human-centered computer security in the nuclear sector. Findings of this nature motivate the need for continued engagement from the IAEA to support Member States in the development of nuclear sector-specific training, as proposed in Resolution GC(62)/RES/7.

The paper concludes with recommendations both for the design of requirements gathering processes and improved computer security training and exercises in the nuclear sector. To advance computer security education in this field, different approaches should be considered, according to their applicability for the individuals using them: For both theory-driven and hands-on computer security education, participants preferred scenario-based approaches, followed by game-based approaches for knowledge and awareness building, and by field exercises for practical application. Ranking key factors showed that industrial control system considerations and implementing computer security incident response plans should be addressed within the next larger training activities. A further aspect that became apparent is that awareness and knowledge building measures should be consistently evaluated, in a similar way as is already common for practical exercises.

The research leading to these results has received funding from the IAEA as part of the CRP J02008 on Enhancing Computer Security Incident Analysis at Nuclear Facilities.

Gender

State

Austria

Primary authors: Ms REISINGER, Michaela (AIT Austrian Institute of Technology); Dr FRÖHLICH, Peter (AIT Austrian Institute of Technology); SMITH, Paul (AIT Austrian Institute of Technology); HEWES, Mitchell (IAEA)

Presenters: Ms REISINGER, Michaela (AIT Austrian Institute of Technology); Dr FRÖHLICH, Peter (AIT Austrian Institute of Technology); SMITH, Paul (AIT Austrian Institute of Technology)

Track Classification: CC: Information and computer security considerations for nuclear security