Contribution ID: **272** Type: **Interactive Content Presentation**

Increasing Computer Security for Radiological Facilities

Increasingly, physical security systems are evolving from analog, hardwired equipment to digital, networked, Internet Protocol (IP)-based components which means that computer security must be considered when implementing physical security upgrades to protect radiation sources. The blending of physical protection systems with traditional information technology systems is advancing at such a rapid pace that the two can no longer be viewed independently or separately. Security systems are evolving from standalone hardwired devices to network-based devices where both power and data may be provided by a single Ethernet cable.

Radiological facilities have a challenge to stay abreast of the threat while accurately assessing computer security threats related to physical security systems protecting radioactive sources, mitigating the risks, and sustaining risk reduction. The primary computer security concern that face radiological facilities are an adversary who could use a cyber-attack to override a facility's existing network controls and physical security measures, allowing them to facilitate a physical attack that could result in unauthorized and/or undetected access to radioactive sources.

The protection of radiological materials is covered in the IAEA's NSS 11 (Security of Radioactive Sources) and NSS 17 (Computer Security at Nuclear Facilities) can provide users of radioactive sources with helpful information on computer security concepts and higher-level responsibilities, but it doesn't give specific guidance on the specific computer security controls that a radiological facility should implement. It is also not sized appropriately for typical sites which have radiological sources. The ORS Cybersecurity Best Practices for Users of Radioactive Sources fills this void by recommending measures for developing a computer security program, implementing specific computer security controls appropriate for a radiological facility, and provides recommended measures to sustain the computer security program. To address these security concerns, ORS has developed a Cybersecurity Best Practices for Users of Radioactive Sources. The ORS best practices guide provides an overview of how physical protection systems have computer security issues and covers recommended best practices for sites to improve their computer security posture with a focus on computer security hygiene measures. The intended users of the best practices guide are regulators, site security officers, site management, and security vendors. Users of radioactive sources that are part of large organizations such as research institutes, universities, medical facilities, or large companies may have computer security programs. The best practices guide is geared towards users of radioactive sources with limited computer security experience to provide information for countering potential cyber threats to their radiological facilities.

We will discuss progress and capabilities of the ORS cybersecurity program. Training, awareness, and best practices are key to this program. So is enhancing the security configuration of installed equipment, and enhancing the environment that equipment installed into. We will discuss key accomplishments of the program and its impact on both domestic and international sites. Active collaborations with industry, regulators and international organizations will be described. Our future plans to implement continuing process improvement will be delineated.

Gender

Male

State

United States

Authors: Mr BUTLER, Nicholas (U.S. Department of Energy/National Nuclear Security Administration); HERDES, Gregory (NNSA Office of Radiological Security); WHITE, Greg (Lawrence Livermore National Laboratory)

Presenter: Mr BUTLER, Nicholas (U.S. Department of Energy/National Nuclear Security Administration)

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