Contribution ID: **564** Type: **Paper**

Examining Cyber Security Vulnerabilities and Counter-Measures to Combat the Insider Threat in Radiological Security

The U.S. Department of Energy/National Nuclear Security Administration's Office of Radiological Security (ORS) collaborates with partner countries throughout the world to enhance the security of radioactive sources used for legitimate purposes. The partner stakeholders' environments consist of operators utilizing ionizing radiation for medical, industrial, and research applications. In each of those domains, the risk of an insider is ever-present within the spectrum of threats and threat agents. With the continued advancement of security technology and the proliferation in the use of networked security components in recent years, previously unforeseen capabilities are being leveraged by security practitioners to greatly enhance detection, assessment, and response security functions. However, as systems increase in the level of integration and complexity, such as those either connected to or riding directly on a site's Information Technology (IT) network, those same security practitioners must also remain vigilant of the associated risks. IAEA Nuclear Security Series No. 11, Security of Radioactive Sources, outlines security objectives for the various security functions of detection, delay, and response. NSS-11 also emphasizes the importance of understanding the threat environment, including the threat posed by the insider, by conducting a vulnerability assessment at a site. Due to the purposes for which radioactive materials are used in several common application spaces, such as medical treatment, academic research, and industrial applications that emphasize process throughput, the quantity of people who have access to the source (whether escorted or unescorted) presents a security management challenge. As the security components become further networked and interrelated, satisfying the recommendations of NSS-11 necessitates a greater emphasis be placed on insider mitigation through the strategic identification, selection, and implementation of administrative, technical, and physical controls to address the cyber vulnerabilities.

To ensure detection of unauthorized attempts to access the radiological source and to counter the insider threat in an environment where it is challenging to limit access to the source, it is necessary to seek new countermeasures. Technological solutions continue to become increasingly affordable, leading to new options for augmenting source security and improving sites' ability to address IAEA recommendations regarding security management and access control, as well as the security fundamental of adversary detection. Unfortunately, as security measures evolve, so does an adversary's capability to defeat those measures. Off-site monitoring of security alarms provides some assurance that an insider's attempts to gain unauthorized access to the source will be detected and a response initiated. Off-site monitoring is, in its turn, dependent upon reliable communications via a variety of channels that may include telephonic, internet, and cloud-based options.

Because of the networked nature of security system hardware and the need for reliable communication to be effective, security system design and deployment must consider physical security from a cyber-security perspective. Key first steps include a range of procedural and practical measures to close fundamental gaps in cyber security and enable the successful employment of networked security systems to prevent malicious acts. Establishing multiple channels of communication, as well as the standard defense-in-depth approach to security system design combine to mitigate the threat posed by a cyber-based attempt to thwart the security system, as well.

NSS-11 identifies the security functions of detection, delay, and response to be addressed by an effective security systems to address the threats to radioactive sources. The recommended response objectives captured in Table 2 of the document hinge on provision of immediate response to an alarm in order to satisfy the recommended requirements. In its interaction with responders to improve response capabilities, expediting data flow to the responders themselves is frequently identified as a mechanism to satisfy those requirements. In the course of collaboration, ORS has striven to identify a mechanism to further fortify the mechanisms for ensuring data flows expeditiously to necessary response personnel. One solution being explored is the development of a cloud-based architecture to streamline communications, ensure delivery of alarm notifications and key data, and ultimately optimize the response timeline and maximize the possibility of interrupting the adversary. This paper will specifically survey the challenges posed by the cyber vulnerabilities at the facilities using radiological sources, the measures identified to mitigate those challenges, and the persistent problem areas that still demand solutions. Additionally, the paper will specifically survey the cyber-security challenges posed by the use of the cloud-based solutions being explored to optimize the ability of sites and responders to achieve the security objectives defined in NSS-11 regarding detection, delay, and response to malicious attempts to access a radioactive source.

Gender

Female

State

United States

Primary author: Ms WISE, Jaime (Pacific Northwest National Laboratory)

Co-authors: HAZEL, Michael (Pacific Northwest National Laboratory (US Department of Energy)); Mr GORTON, Brandon (Pacific Northwest National Laboratory); Mr HIGGINS, Brian (Pacific Northwest National Laboratory)

Presenter: HAZEL, Michael (Pacific Northwest National Laboratory (US Department of Energy))

Track Classification: PP: Insider threats