World Institute for Nuclear Security

Round Table on Cybersecurity Best Practices for Users of Radioactive Sources

Vienna, Austria. 10 - 11 September 2019

Round Table on Cybersecurity Best Practices for Users of Radioactive Sources

Vienna, Austria. 10 – 11 September 2019

BACKGROUND

Radioactive sources benefit human beings in a wide variety of ways—from medicine and industry to agriculture and research. However, they also have the potential to cause great harm if they are not properly managed. As the threat from terrorism has grown in the last decades, the awareness that radioactive sources can potentially pose a serious security risk has also grown. As a result, States and regulatory bodies have instituted new regulations and other mechanisms to mitigate this risk.

In response to the threat and in compliance with regulatory requirements, end users have established security programmes for their radioactive materials. The security systems implemented at the facility level have been mostly designed to deter and respond to physical attacks conducted by outsiders, including criminals and terrorists, and by employees and other individuals authorised to physically access the premises where sources are in use or storage (insiders).

One of the greatest challenges in this regard is security's increasing reliance on digital technology at every level. For example, many elements of the physical protection systems now rely on digital technologies and associated IT infrastructures—from operations and communications to alarm monitoring stations and fundamental elements of the intrusion detection, access control and alarm assessment systems. If not properly protected, these elements are vulnerable to cyberattacks that could degrade the performance of the physical protection systems and lead to vulnerabilities in the security of the radioactive sources themselves.

Social engineering attacks, such as phishing emails, are a major cause for concern because they can give adversaries remote access to physical protection systems and the IT infrastructure. Another challenge is that end users store a variety of sensitive information on IT systems that could compromise radioactive source security.

This includes information related to the security plan, access codes and alarm system codes/ passwords.It also includes source inventory (including locations and amounts), operational procedures, computer systems, transport timing and routes, technical data, blueprints, schematics, designs, security procedures and emergency response plans. Such information requires protection against unauthorised disclosure.

End users may also possess business sensitive data, customer-related materials and patient health records whose disclosure could lead to negative competitive business impacts or significant liabilities for the organisation. In addition, processes that use sources or devices that contain sources might also become the target of cyberattacks that could disrupt facility operations, lead to loss of production, damage customers or adversely impact patient health.

A particular challenge for the health care industry is that medical devices are increasingly connected to the internet, hospital networks, and other medical devices to provide remote diagnostics and features that increase the ability of health care providers to treat patients. However, such features also increase cybersecurity risk. Furthermore, medical devices, like other computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device itself .

Round Table on Cybersecurity Best Practices for Users of Radioactive Sources

Vienna, Austria. 10 – 11 September 2019

OBJECTIVES

Understanding and mitigating the cybersecurity risk associated with radioactive sources is especially challenging. WINS has therefore decided to conduct a 2-day event that will bring experts together to identify the magnitude of this risk and to review best practices for establishing effective cybersecurity programmes at end users' facilities.

The Round Table will give participants the opportunity to:

- Identify the cybersecurity risk as it relates to the management of radioactive sources, especially the potential impact of cyberattacks on physical protection systems
- Review the international recommendations and guidance on the topic and discuss mechanisms to increase awareness amongst radiological security stakeholders
- Review the key elements and attributes of an effective cybersecurity programme
- Understand the need for manufacturers, end-users, regulators and security experts to work together to manage cybersecurity risks
- Listen to the experience and lessons learned from experts and organisations that have designed and implemented cybersecurity measures for radioactive sources
- Identify and consolidate best practices for designing and implementing a cybersecurity programme related to radioactive sources
- Develop a way forward to raise awareness amongst end-users and contribute to the strengthening of cybersecurity for radioactive sources.

WINS World Institute for Nuclear Security

Round Table on Cybersecurity Best Practices for Users of Radioactive Sources

Vienna, Austria. 10 - 11 September 2019

TARGETED AUDIENCE

- Representatives of organisations that use high activity radioactive sources (medical, academic and industry);
- Representatives from source producers and suppliers;
- Representatives from regulatory authorities and law enforcement agencies;
- Cybersecurity experts, consultants and vendors;
- Physical security experts, consultants and vendors; and
- Representatives from professional associations and international organisations or support programmes.

EVENT PROCESS

The framework for the round table will consist of presentations and plenary and group discussions. The round table will be conducted in English and draw only on unclassified information.

Participation will be limited. Attendees will be expected to meet their own costs for travel and accommodation, but the organisers will meet all event costs. No registration fee is required.

LOCATION

Arcotel Kaisserwasser
Vienna, Austria

DATE

10 - 11 September 2019