World Institute for Nuclear Security

Round Table on Cybersecurity Best Practices for Users of Radioactive Sources

Vienna, Austria. 10-11 September 2019

Agenda - As of 05 September 2019

DAY 1: TUESDAY 10 SEPTEMBER 2019

08:30 – 09:00 Registration / Coffee & Tea

OPENING SESSION

09:00 – 09:15 Welcome & opening remarks (Pierre Legoux, WINS)

09:15 – 09:45 Participants introduction and review of expected outcomes (Anna Patterson, Facilitator)

09:45 – 10:15 **Cyber Threats and Radiological Security Risk**
Presentation by Jessica Fahey, Canadian Nuclear Safety Commission (CNSC), Canada

10:15 – 10:30 **Discussion** to develop a common understanding
- What do we mean by cyber threats and cybersecurity?
- How does the topic relate to radioactive sources and other practices involving radiation?
- Why is it important to address this issue? What consequences could arise from a cyber attack?

10:30 – 10:45 Coffee Break

SESSION 1: UNDERSTANDING CYBER THREATS AND ASSOCIATED RISKS FOR RADIOACTIVE SOURCES

Key issues:
- How can cyber threats be characterised? How do cyber threats differ from or complement other types of threats?
- What are actual examples of cyber attacks that impact the security of radioactive sources? Are blended physical and cyber attacks against radioactive sources credible?
- What evolution in the threat landscape can we expect in the future?

10:45 – 11:15 **Cyber threats – Attributes and characteristics**
Presentation by Marina Krotofil, BASF, Germany

11:15 – 12:15 **Break out groups** on
- Credibility and likelihood of the threat
- Actual attack examples and hypothetical scenarios of concern
- Good practices for transferring cyber threats information to those who need to know

12:15 – 13:15 Lunch

SESSION 2: PROTECTING PHYSICAL SECURITY SYSTEMS AGAINTS CYBER ATTACKS

Key issues:
- Why are cyber threats a concern for physical security systems?
- What are good practices for protecting security systems against cyber attacks?
- What are we good at? What might be remaining vulnerabilities?

13:15 – 14:15 **Cyber attacks of selected physical security equipment**
Presentation by Paul Smith and Ewa Piatkowska, Austrian Institute of Technology, Austria

14:15 – 14:45 **Cybersecurity Best Practices for Users of Radioactive Sources**
Presentation by Greg Herdes, DOE/NNSA Office of Radiological Security, USA

14:45 – 15:15 **Discussion** to share experiences and lessons learned in designing and implementing cybersecurity measures to support physical security systems

15:15 – 15:30 Coffee Break

SESSION 3: CYBER SECURITY FOR RADIATION DEVICES

Key issues:

- Why are cyber threats a concern for radiation devices?
- What are good practices for protecting radiation devices against cyber attacks?
- What are we good at? What might be remaining vulnerabilities?

15:30 – 16:45 **Strengthening the cyber security of equipment containing radioactive sources**

- **Presentations on medical applications**
  - Elizabeth Nichols, University of Maryland, USA (remote presentation)
  - Nicholas Hakamaki, Best Theratronics, Canada
- **Discussion on industrial applications**
  - Leigh Catley, Nordion, Canada

16:45 – 17:15 **Plenary and Table Discussion** to share further experiences and lessons learned from on-going efforts to strengthen the cybersecurity of radiation devices

17:15 – 17:30 Review of the day – Key findings and main take-away

17:30 Event Reception

DAY 2: WEDNESDAY 11 SEPTEMBER 2019

09:00 – 09:30 Review of Day 1 (Facilitator)

SESSION 4: DEVELOPING A COMPREHENSIVE APPROACH TO CYBERSECURITY

Key issues:

- What are the respective roles and responsibilities in mitigating cyber threats?
- What are the key elements and attributes of a comprehensive cybersecurity programme?
- What can we learn from those who are implementing cyber security arrangements?

09:30 – 10:30 **Group Discussion** to identify and discuss roles and responsibilities for mitigating cyber threats

- Who are the main stakeholders?
- What is their expected contribution?
- How satisfied are we of their contribution?

10:30 – 10:45 Coffee Break

SESSION 5: RAISING CYBERSECURITY AWARENESS AMONGST KEY STAKEHOLDERS

Key issues:

- How do we know that our cybersecurity arrangements are efficient?
- How can we raise security awareness and competencies amongst key stakeholders? What could be relevant regulatory cyber security requirements for radioactive sources?
- What should our priorities be?

10:45 – 11:15 **International efforts to support the development of recommendations and guidance for the cyber security of radioactive sources**
Presentation by Trent Nelson, IAEA Nuclear Security Division

11:15 – 11:30 **Discussion** on best approaches for raising awareness amongst stakeholders

11:30 – 12:00 **3D Hospital Model for cybersecurity training**
Presentation by Greg White, Lawrence Livermore National Laboratory, US

12:00 – 12:30 **Discussion** on how to identify necessary competences for the people involved in the cyber security of radioactive sources and provide them with necessary education and professional development opportunities

12:30 – 13:30 Lunch

CONCLUSION SESSION

13:30 – 14:30 **Way Forward**

- What are the key lessons that have arisen from this round table? What are main our take-aways?
- What questions and challenges remain unaddressed?
- How can we ensure a follow-up to the key findings?

14:30 – 15:00 **Round table evaluation and closing remarks**