# Round Table on Cybersecurity Best Practices for Users of Radioactive Sources

# Vienna, Austria. 10- 11 September 2019

# REPORT

# (Preliminary draft for comments and technical edition)

## 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.

## OBJECTIVES OF THE ROUND TABLE

The key objectives of the round table were to provide participants with 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.

Twenty-eight experts from nine countries and four international organisations attended the round table. They represented the main stakeholders involved in the cyber security of radioactive sources used in medical and industrial applications (i.e. end users, regulators, device manufacturers, international support programmes and cyber security professionals). Participants were expected to have open discussions, express their own perspectives and offer suggestions for increasing cyber security awareness amongst radioactive source practitioners and for strengthening cyber security arrangements for radioactive sources.

The event, which was professionally facilitated by Ms Anna Patterson, included expert presentations and plenary and breakout sessions to provide maximum engagement. In addition, an instant electronic voting system was used to allow participants to anonymously share their views on selected questions. Some e-voting questions are reflected in this report.

## ROUND TABLE PROGRAMME AND KEY FINDINGS

**DAY 1: TUESDAY 10 SEPTEMBER 2019**

## OPENING SESSION

**Mr Pierre Legoux, WINS Head of Programmes**, welcomed the participants on behalf of WINS, detailed the objectives of the round table and provided a preliminary overview of the agenda. Mr Legoux also displayed and commented on the most relevant results from the pre-event survey.

Participants’ expectations

Participants were asked to introduce themselves at their tables and discuss their expectations coming into this event. Some examples include:

* Share experiences. Network. Increase knowledge;
* Understand what others do. Benchmark our practices;
* Receive information about the latest developments regarding cyber security of radioactive sources and feedback it to my colleagues;
* Express my needs and challenges. Explore possible solutions, not just admire the problem;
* Identify possible gaps. Review options to develop comprehensive and consistent approaches;
* Better understand options to raise cybersecurity awareness.

Keynote presentation on Cyber Threat and Radiological Security Risks

**Ms Jessica Fahey, CNSC (Canada)** offered an opening perspective on the various elements of the round table agenda. After summarising the mandate of the CNSC and the list of activities regulated by her organisation, Ms Fahey provided a definition of cyber threats, a review of cyber threat actors and a summary of the implication of cyber threats for radiological security. She then presented the overall Canadian approach to mitigate the risk, detailing in particular the role of the Canadian Centre for Cyber Security and how CNSC was structured to manage the cyber risk and contribute to mitigate it amongst its licensees. Mr Fahey concluded he presentation by describing and insisting on the importance of coordinating efforts at national and international levels.

Discussion on key issues to be kept in mind during the round table

Participants were then asked to hold discussions on why it is important to address the issue of cyber security for radioactive sources and to highlight what could be in their mind some of the key issues to improve the awareness of the cyber security risk and ensure the effectiveness of mitigation measures.

First, participants stressed the need to obtain buy-in from all stakeholders. They indicated that the international community, in particular the IAEA, had started to address the topic and that the industry, especially the device manufacturers, was a leading actor in this area. It was agreed that end users were still struggling on measures to implement and that they would welcome much more directive and guidance from regulatory agencies.

As for many security matters, participants highlighted the leading role of senior management and of the importance of raising their awareness and understanding of the risk. It was mentioned that speaking senior management language and addressing their key expectations, which are often driven by costs and impact of investment, was a prerequisite to their proper engagement.

Participants then discussed the essential role of culture and of the need to develop a robust security culture combining physical and cyber risks. It was mentioned that too often people still believe that the problems will happen to someone else. A lot of individuals still do not understand the risk. Some participants expressed doubt on the effectiveness of the communication and awareness campaigns that have been conducted so far.

Finally, the importance of measuring the effectiveness of cyber security arrangements was discussed. Do we really know where we stand? Are we conscious of our vulnerabilities? It was agreed that measuring the effectiveness of cyber security programmes was still challenging, in particular because key performance indicators for cyber matters are not always intuitive to humans.

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

The objectives of Session 1 were to explore cyber threats, review their characteristics and better understand how they may differ from or complement other types of threats. It was also to review actual examples of cyber-attacks and discuss how it would relate to the security of radioactive sources. The session was also an opportunity to discuss what evolution in the threat landscape could be expected in the future.

E-Voting

To initiate the discussions on cyber threats and help focus on key issues, participants were requested to share their opinion on the communication of threat information to those who need to know. They clearly indicated that in their mind the dissemination of this information is not as efficient as it should be. As possible improvement, participants suggested to clarify what information is needed by each stakeholder and tailor the message. They also suggested to establish exchange groups based on the need-to-know and to build communication mechanisms around them. Participants highlighted the need to build confidence and create groups of trusted people.

**Ms Marina Krotofil, BASF (Germany)** delivered a presentation on *Understanding Cyber Threats and Associated Risks for Radioactive Sources*. First, Ms Krotofil explained how the threat, including terrorist groups, criminals and state-sponsored entities, has evolved in the last few years and will continue to evolve at fast pace in the coming years. Referring to some recent high-profile cyber-attacks she indicated that our protective mechanisms are not as robust as they should be and that adversaries are capable to identify and exploit existing vulnerabilities. Ms Krotofil provided examples of information and equipment that adversaries can easily find on internet to support their malicious goals. She continued her presentation by providing some trends in cyber threats and some details on potential attacks to be expected in the near future. Ms Krotofil concluded her contribution by highlighting the need for ensuring the cyber security of the equipment used in industrial processes and security systems and for paying particular attention to the supply-chain and outsourced services.

Following the presentation, participants had discussions in small groups to further explore the credibility of cyber threats and how they could materialise in their activities. They also discuss how the cyber risk could be reduced. Some of the key findings of the discussions include:

* We are still Incident driven;
* Threat is real and evolves permanently;
* Defensive mechanisms might not be strong enough;
* Ransomware attacks happen frequently;
* Industry would collectively suffer in case of a significant incident;
* Developing a graded approach is required;
* We need to better use CERTs and ISACs.

## SESSION 2: PROTECTING PHYSICAL SECURITY SYSTEMS AGAINST CYBER ATTACKS

Building on the key findings of previous discussions, Session 2 was designed to specifically explore why cyber threats are of concern for physical security systems and to identify best practices for protecting security systems against cyber-attacks.

**Mr Paul Smith and Ms Ewa Piatkowska from the Austrian Institute of Technology** then offered a demonstration describing some potential vulnerabilities of selected physical security equipment to cyber threats. Mr Smith first presented the motivation for digitalisation and provided an explanation why every sector and activity are embarked into this process. He then provided the group with some background and detailed information on the hypothetical medical facility to be used in the scenario supporting the demonstration. The main objective of this demonstration was to identify conditions whereby a threat actor could identify and digitally compromise a security system in order to gain unauthorized access to radioactive sources. Ms Piatkowska and Mr Smith demonstrated live how access control systems and monitoring equipment, such as biometrics devices and CCTV, could be tampered or manipulated to the benefit of adversaries.

As a complementary perspective, **Mr Greg Herdes, Office of Radiological Security, US DOE** provided the group with a presentation on *Cybersecurity Best Practices for Users of Radioactive Sources*. Mr Herdes opened his presentation by describing the evolution of security systems indicating that blending of physical protection systems with IT is advancing at such a rapid pace that the two can no longer be viewed independently or separately. He then summarised the cyber security concerns associated with the use of radioactive sources and offered a detailed description of possible cyber security measures for security equipment. Mr Herdes concluded his presentation by providing further information of the cyber security tools, including best practice guides and training materials, developed by his organisation and how they could effectively support stakeholders willing to enhance their cyber security arrangements.

Group discussion

Reflecting on what they had seen during the demonstration and heard during the presentation, participants were asked to form small groups and to exchange their perspectives on the risk and how to mitigate it. Key messages provided by the various groups were as follows:

* Physical security people are struggling to grasp the problem;
* There is a need to make the cyber robustness of physical security equipment more “visual”;
* Supply chain and outsourcing create challenges;
* Vendors should be encouraged to provide “hardened” devices;
* Are there actual examples of cyber-attacks of PPS (of rad sources)?
* Conduct penetration testing. Red teaming including both cyber and PP exists;
* What are the performance expectations/design inputs of the equipment composing the PPS? Is there a role for a Design Basis Threat?
* It is already challenging to maintain PP up to date. Adding the cyber layer is even more challenging;
* You need a “Champion” to bring all the pieces of the puzzle together.

## SESSION 3: CYBER SECURITY FOR RADIATION DEVICES

Session 3 was designed to review what could be cyber threats for radiation devices and to better understand what possible security measures for protecting these devices against cyber-attacks could be. It was in particular to review what has already been achieved in term of cyber security of devices and identify what could be remaining vulnerabilities.

Session 3 was opened by a remote presentation (Skype) delivered by **Ms Elizabeth Nichols, University of Maryland, USA**. Referring to an incident that occurred in 2016 and other factors, Ms Nichols first explained why cybersecurity was of high importance for her organisation. She then highlighted some of the usual challenges faced by the medical sector when trying to enhance cyber security arrangements. Ms Nichols continued her presentation by explaining how cyber security relate to radiation oncology matters and how issues with hardware or software elements of the medical devices may prevent her organisation to deliver expected medical treatments. Highlighting some of the keys to success to establish robust cyber security programmes at medical facilities and the usual challenges with cybersecurity in the healthcare sector, Ms Nichols concluded her presentation by providing a summary of the experience and key findings of the efforts of the University of Maryland to improve cyber security arrangements.

Complementing the end-user perspective provided by Ms Nichols, **Mr Nick Hakamaki, Best Theratronics, Canada** offered a Manufacturer perspective. Mr Hakamaki started his presentation by a brief introduction of Best Theratronics and of its main products. He then explained why cyber security is an important topic for Best, in particular how cyber security matters relate to Best’s activities and equipment, and what the main scenarios of concern are for Best. Mr Hakamaki described some of the protective measures in place and explained how Best and other stakeholders are increasing their coordination and cooperation to tackle the problem together. He concluded his presentation by providing some insights on what upcoming threats could be and how next generation of firewalls may assist to mitigate the risk.

As final contribution to the topic, Ms Patterson facilitated a discussion with Leigh Catley who is the Senior Director IT Governance and Security at Nordion in Canada. The discussion topics included questions on risk perception and how to communicate the threat information to the staff, and on risk mitigation and the essential elements of a comprehensive mitigation programme. They also included the role and contribution of various stakeholders with a focus on customers expectations and the role of regulatory agencies.

Group discussion

In a similar manner to Session 2, participants were asked to form small groups to share their reactions to what they had heard from the three contributors and consolidate their perspective and key messages for enhancing the cyber security of radiation devices. Key outputs from these discussions were:

* It is difficult to understand what is cyber when you are not an expert. Too many people still wait for an incident to do something. Bad experiences are strong incentives to improve but they can do a lot of damages. Regulations can anticipate a problem;
* Remote access (e.g. maintenance or diagnosis) creates risks. Availability of the IP address make it reachable from anywhere in the world. Even protected, an access remains an access;
* It is difficult to bring all the computers/devices up to date at the same moment. Some updates may require recommissioning of medical devices;
* Unwilling insider is of key concern. Staff is often not aware they can be used to “support” a cyber-attack;
* Air gaps do not exist. A proper one would mean no modification at all;
* Disable as many ports as possible. Make unauthorized communication as difficult as possible
* “Cyber security” of a device degrades overtime and operators need to have a continuous assessment and improvement process in place.
* Safety first, then security, then cyber. It is a long journey

## SESSION 4: DEVELOPING A COMPREHENSIVE APPROACH TO CYBERSECURITY

Session 4, the first session of the second day of the round table, was organised to identify the key stakeholders for mitigating cyber risks for sources, review their expected role and assess their level of contribution to developing a comprehensive cybersecurity programme.

E-Voting

In order to initiate the discussions, the participants were asked to answer an e-voting question on the awareness of the various stakeholders and of their coordination and cooperation. Participants expressed mix-feelings and a need for improvement. It was clear that some stakeholders, such as industry, were aware of the risks and proactive in their actions, while some others, such as licensees, were often lagging behind and still struggling on what was expected from them and on what to achieve.

In a presentation titled *Guidance Development on Computer Security for Other Radioactive Material*, **Mr Trent Nelson from the IAEA** detailed first the large range of IAEA activities available to support Member States to develop effective information and computer security arrangements for their programmes involving nuclear and other radioactive materials. Mr Nelson then focused on NSS 14 dealing with the protection of radioactive materials and on the development of a new guidance document that will specifically address the cyber security of these materials. He concluded his presentation by highlighting the key upcoming IAEA meetings and activities related to computer security for nuclear security matters.

Group discussion

Participants were then asked to form sub-groups and first to identify and characterise the key stakeholders (Who are they? What are their responsibilities and contribution? What relationships do they have? How intensive are these relationships?). Participants were also asked to discuss what motivates each stakeholder and how the difference in motivations was impacting the implementation of effective cyber security.

As final activity of Session 4, a plenary discussion was organised to reflect on the key findings of the group discussion for the regulatory and explore challenges in the relationship between regulators and end users, in particular when it relates to developing new regulatory requirements.

## SESSION 5: RAISING CYBERSECURITY AWARENESS AMONGST KEY STAKEHOLDERS

The last session of the round table was organised to identify and discuss good practices for raising cybersecurity awareness and increasing competencies amongst key stakeholders.

**Mr Greg White from Lawrence Livermore National Laboratory (LLNL), USA** presented the use of a 3D hospital model for cybersecurity training purpose. Mr White started his presentation by explaining the need for hypothetical facilities in training curriculum. In particular he described the Shapash Nuclear Research Institute which is used by the IAEA and the US DOE in their cybersecurity training courses. Mr White also explained how 3D models cab enhance the training experience and then provided more details on the Gula Regional Hospital the DOE will use in the future to simulate the impact of a cyber-attack on physical protection systems as part of a blended attack and as training tool to support the implementation of the ORS cybersecurity best practices.

Group discussion

Following the presentation, participants were then asked to discuss what are the main challenges to raise cyber security awareness for radioactive sources. They were also asked to discuss necessary competences for the individuals in charge of cyber security and draft a hypothetical job description to be used for the recruitment of a new person in charge of the cyber security of radioactive sources. Their key findings were as follows:

**Challenges to raising cyber security awareness**

* It is difficult to articulate cyber security matters into usual business language.
* Many cyber security reports and communication moments are already existing but almost none are directly related to radioactive source security.
* Too many reports may dilute the key messages.
* Many people still do not feel at risk. Some organisations do not feel as a target due to their size or type of business. No incident has happened, what should they bother?
* Convert high media attention to individual cases.
* There is also a global lack of (cyber) security culture and many organisations face resistance to change.

**Challenges to developing and retaining necessary competences**

* There is a lot of confusion between IT skills and cyber security skills. They do not mean the same and require different competencies.
* Developing competencies cost money (direct cost and staff cost)
* Due to the high demand for competent staff it is difficult to keep well trained, efficient IT security staff.
* Make developing competences a corporate priority. Allocate necessary resources.
* Do not wait for regulatory guidance on competences, develop your own competence matrix
* Pay well your qualified staff.
* Perform root cause analysis for problems or unsatisfactory situations. Look at leading companies.

## WAY FORWARD AND CONCLUSION

As last activity of the round table, participants were asked first to define personal commitments towards concrete steps supporting the enhancement of cyber security in their organisation or sector and to share them with other representatives of their stakeholder groups (end users, industry, regulators, international organisations, etc.). Participants were then encouraged to discuss as a whole group the main findings of the event and share some of their take-aways and possible follow up actions.

Examples of findings of the event include:

* There is a momentum. Individuals start to be more conscious of the risk. Improvements are on the way. There is an appetite for progress out there;
* Global awareness is increasing. International community is taking the problem seriously. International Guidance and training are under development;
* We already have measures in place. There is a lot of on-going R&D for defensive security;
* It is more and more common to talk about PP and cyber together;
* We have good records of managing sources. We can build on this. We have a culture of continuous improvement;
* We have achieved good stuff. We do not want to lose these achievements;
* We are developing integrated risk management approaches. Team work is encouraged at all levels;
* Resources start to be available. Experts are available to answer questions.

In his concluding remarks, Mr. Legoux thanked participants for their active contributions during the round table, which made the event a success. He encouraged them to continue exchanging their ideas and experiences in enhancing the cyber security of radioactive sources. He also committed WINS to building on this success, to update WINS publications on radiological security to increase guidance on cyber security matters, and to continue offering opportunities for information exchange and professional development to all stakeholders involved in the security of radioactive sources.

During the evaluation session, 100% of the attendees expressed satisfaction with the event and of the facilitation process and 88% of the attendees indicated they would recommend this type of event to others. In their individual comments, participants confirmed a high level of satisfaction and said they particularly valued the amount of information shared during the two days, the atmosphere of trust and the networking opportunities. They finally encouraged WINS to ensure a broader diversity of countries attending this type of events.