World Institute for Nuclear Security

Round Table on Cybersecurity Best Practices for Users of Radioactive Sources

Vienna, Austria. 10- 11 September 2019

REPORT

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 could 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 (i.e. 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 physical protection systems (PPS) now rely on digital technologies and associated information technology (IT) infrastructures—including operations, communications, alarm monitoring, 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 PPS 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 PPS 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 and significant liabilities for the organisation. In addition, processes that use sources or devices that contain sources might also become the target of a cyberattack that could disrupt facility operations, lead to loss of production, damage customers or adversely impact patient health.

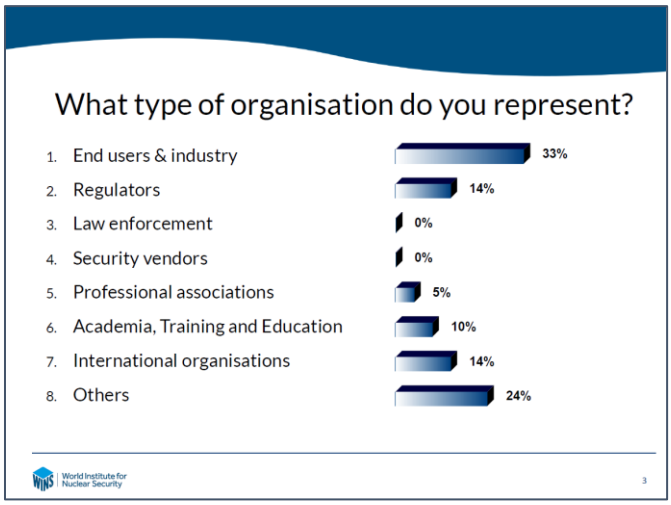
A particular challenge for the health care industry is that medical devices are increasingly connected to the internet, hospital networks, and other medical devices to provide remote diagnostics and features that increase the ability of health care providers to treat patients. However, such features 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 cybersecurity risk as it relates to the management of radioactive sources, especially the potential impact of cyberattacks on PPS.
- 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 cybersecurity of radioactive sources used in medical and industrial applications (i.e. end users, regulators, device manufacturers, international support programmes and cybersecurity professionals).



Participants were expected to have open discussions, express their own perspectives, and offer suggestions for increasing cybersecurity awareness amongst radioactive source practitioners and for strengthening cybersecurity 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 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 included:

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

Keynote presentation on cyberthreat and radiological security risks

Ms Jessica Fahey, Canadian Nuclear Safety Commission (CNSC), offered an opening perspective of various elements of the round table agenda. She began by summarising CNSC's mandate and the activities it regulates. Then she defined what is meant by cyberthreats, reviewed cyberthreat actors, and summarised the implications of cyberthreats for radiological security. She also presented Canada's overall approach to mitigating risk, detailing in particular the role of the Canadian Centre for Cybersecurity and how CNSC is structured to manage the cyber risk and help licensees mitigate it. Ms Fahey concluded her presentation by emphasising the importance of coordinating efforts at the national and international level.

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

Participants were then asked to discuss among themselves why it is important to address the issue of cybersecurity for radioactive sources and to identify some of the key issues involving risk awareness and the effectiveness of mitigation measures.

Participants emphasised the need to obtain buy-in from all stakeholders. They said that the international community, in particular the IAEA, has started to address the topic and that the industry, especially device manufacturers, is a leading actor in this area. They also said that end users are still struggling with which measures to implement and would welcome much more directive guidance from regulatory agencies.

In addition, participants emphasised the leading role of senior management when it comes to security matters and of the importance of raising their awareness and understanding of the risk. Participants also mentioned that to engage with management effectively it is necessary to address their key expectations, which are often driven by costs and the impact of investment.

Participants then discussed the need to develop a robust security culture that combines physical and cyber risks. They mentioned that many people still do not understand the risk and believe that problems only happen to others. Some said that the communication and awareness campaigns that have been conducted so far are ineffective.

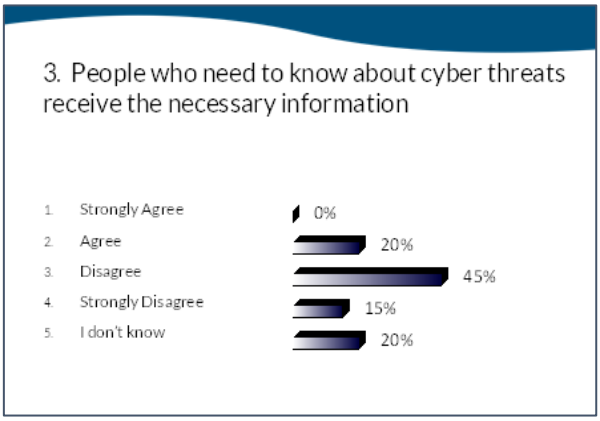
Finally, participants also discussed the importance of measuring the effectiveness of cybersecurity arrangements. Do we really know where we stand? Are we conscious of our vulnerabilities? Some participants mentioned that it is challenging to measure the effectiveness of cybersecurity programmes, especially because key performance indicators for cyber matters are not always intuitive to humans.

SESSION 1: UNDERSTANDING CYBERTHREATS AND ASSOCIATED RISKS FOR RADIOACTIVE SOURCES

The objectives of Session 1 were to explore the characteristics of cyberthreats and how they may differ from and/or complement other types of threat. The session also reviewed actual examples of cyberattacks and discussed how they relate to the security of radioactive sources. In addition, the session gave participants an opportunity to discuss how the threat landscape might evolve in the future.

E-Voting

To initiate the discussions on cyberthreats and focus on key issues, participants were asked to share their opinions about how effectively threat information is being communicated to people who need to know. The results indicate that such communications are not as effective as they should be.



As a possible means of improvement, participants suggested clarifying the information that each stakeholder needs to know and providing such information to each one accordingly. They also suggested establishing exchange groups based on need-to-know and building communication mechanisms around such groups. In particular, they emphasised the need to build confidence and create groups of trusted people.

Ms Marina Krotofil, BASF (Germany), delivered the first presentation of Session 1 titled *Understanding Cyberthreats and Associated Risks for Radioactive Sources*. She explained how the threat, including terrorist groups, criminals and state-sponsored entities, has evolved in the last few years and will continue evolving rapidly in the coming years. In reference to some recent high-profile cyberattacks, she indicated that our protective mechanisms are not as robust as they should be and that adversaries are capable of identifying and exploiting existing vulnerabilities.

In addition, Ms Krotofil provided several examples of information and equipment that adversaries can easily find on the internet to support their malicious goals. She also identified trends in cyberthreats, including potential attacks that can be expected in the near future. She concluded her presentation by emphasising the need to ensure the cybersecurity of the equipment used in industrial processes and security systems—with particular attention paid to the supply chain and outsourced services.

Following the presentation, participants moved into small groups to further explore the credibility of cyberthreats, including how such threats could materialise in their activities. They also discussed how the cyber risk could be reduced. Some key findings include:

- We are still incident-driven.
- The 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 computer emergency response teams (CERTs) and information sharing and analysis centers (ISACs).

SESSION 2: PROTECTING PHYSICAL PROTECTION SYSTEMS AGAINST CYBERATTACK

Building on the key findings of previous discussions, Session 2 was designed to specifically explore why cyberthreats are of concern for physical protection systems (PPS) and to identify best practices for protecting them against cyberattack.

Mr Paul Smith and Ms Ewa Piatkowska, Austrian Institute of Technology, demonstrated some of the potential vulnerabilities of physical protection equipment to cyberthreats using a hypothetical scenario focused on a medical facility. Mr Smith began the presentation by discussing the motivation for digitalisation and why every sector and activity have embarked on this process. He then provided detailed information about the hypothetical medical facility. The main objective of the demonstration was to help participants understand the conditions whereby a threat actor could identify and digitally compromise a security system to gain unauthorized access to radioactive sources. Ms Piatkowska and Mr Smith illustrated 'live' how adversaries could tamper with access control systems and monitoring equipment, such as biometrics devices and CCTV.

Mr Greg Herdes, Office of Radiological Security, US DOE, provided a complementary perspective in his presentation titled *Cybersecurity Best Practices for Users of Radioactive Sources*. He described the evolution of security systems, explaining that the 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 also addressed cybersecurity concerns that are associated with the use of radioactive sources and possible cybersecurity measures that can be applied to security equipment. Mr Herdes concluded his presentation by describing information that DOE has developed, including best practice guides and training materials, for stakeholders who seek to enhance their cybersecurity arrangements.

Group discussion

Participants were then asked to form small groups so they could exchange their perspectives on the risk and how to mitigate it. Key conclusions from the groups included:

- 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 cyberattacks of PPS (of rad sources)?
- It is important to conduct penetration testing. Red teaming that includes both cyber and physical protection (PP) exits.
- What are the performance expectations/design inputs of the equipment that composes the PPS? Is there a role for a design basis threat?
- It is already challenging to keep 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: CYBERSECURITY FOR RADIATION DEVICES

Session 3 was designed to review possible cyberthreats for radiation devices and to better understand security measures that might protect these devices against cyberattacks. In particular, the goal was to review what has already been achieved in terms of the cybersecurity of devices and identify what kind of vulnerabilities remain.

Ms Elizabeth Nichols, University of Maryland, USA, opened Session 3 via a remote presentation (Skype). She described an incident that occurred at the university in 2016 to illustrate why cybersecurity is so important for her organisation. She then described some of the challenges typically faced by the medical sector when trying to enhance cybersecurity arrangements. She also explained how cybersecurity relates to radiation oncology matters and how issues with the hardware or software elements of medical devices could potentially keep a health care facility from delivering the expected medical treatments. In conclusion, Ms Nichols highlighted some of the keys to success in establishing a robust cybersecurity programme at a medical facility and summarised some of the University of Maryland's key findings for improving its cybersecurity arrangements.

Complementing the end user perspective provided by Ms Nichols, **Mr Nick Hakamaki, Best Theratronics, Canada,** offered a manufacturer perspective. Mr Hakamaki began with a brief introduction to his company and its main products. He then explained why cybersecurity is an important topic for Best, in particular how cybersecurity matters relate to its activities and equipment and its main scenarios of concern. 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. Finally, he provided some insights about potential upcoming threats and how the next generation of firewalls may help to mitigate the risk.

Ms Patterson then facilitated a discussion with **Leigh Catley, Senior Director, IT Governance and Security at Nordion (Canada)**. Discussion topics included risk perception and how to communicate threat information to staff. They also included risk mitigation and the essential elements of a comprehensive mitigation programme, as well as the roles of various stakeholders. A major focus of the discussion was on customer expectations and the role of regulatory agencies.

Group discussion

Participants were again asked to form small groups to share their reactions to what they had heard from the three contributors and to consolidate their perspectives and key messages for enhancing the cybersecurity of radiation devices. Key outputs from these discussions were:

- It is difficult to understand what cyber is 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 damage. Regulations can anticipate a problem.
- Remote access (e.g. maintenance or diagnosis) creates risks. Availability of the IP address makes it reachable from anywhere in the world. Even protected, an access remains an access.
- It is difficult to bring all computers/devices up-to-date at the same time. Some updates may require recommissioning of medical devices.
- The unwilling insider is of key concern. Staff are often not aware they can be used to "support" a cyberattack.
- 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.
- The cybersecurity of a device degrades overtime, so operators need to have a continuous assessment and improvement process in place.
- Safety first, then security, then cyber. It is a long journey.

DAY 2: WEDNESDAY, 11 SEPTEMBER 2019

SESSION 4: DEVELOPING A COMPREHENSIVE APPROACH TO CYBERSECURITY

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

E-Voting

To initiate discussions, participants were asked to answer an e-voting question on how aware they think various stakeholders are of their responsibilities for coordinating and cooperating with each other. Participants expressed mixed feelings and a need for improvement. The results make it clear that some stakeholders, such as industry, are aware of the risks and proactive in their actions, whereas others, such as licensees, often lag behind and still struggle with what is expected of them and what they are supposed to achieve.

In a presentation titled *Guidance Development on Computer Security for Other Radioactive Material*, **Mr Trent Nelson, IAEA,** discussed the large range of IAEA activities available to help Member States develop effective information and computer security arrangements for programmes involving nuclear and other radioactive materials. Mr Nelson then focused on NSS 14, which deals with the protection of radioactive materials, and on the development of a new guidance document that will specifically address the cybersecurity 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 in which to identify and characterise the key stakeholders. (Who are they? What are their responsibilities and contributions? What relationships do they have? How intensive are these relationships?). Participants were also asked to discuss what motivates each stakeholder and how this difference in motivation might impact how effectively cybersecurity is implemented.

The final activity of Session 4 consisted of a plenary discussion that enabled participants to reflect on key findings of the regulatory group discussion and to 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 objective of the last session of the round table was to identify and discuss good practices for raising cybersecurity awareness and increasing competencies amongst key stakeholders.

Mr Greg White, Lawrence Livermore National Laboratory (LLNL), USA, demonstrated how to use a 3D hospital model for cybersecurity training purposes. He began by explaining the need for hypothetical facilities in the training curriculum. In particular, he described the Shapash Nuclear Research Institute, which both the IAEA and the US DOE use in their cybersecurity training courses. Mr White explained how 3D models can enhance the training experience and provided details on the hypothetical Gula Regional Hospital. The DOE will use this hospital in the future to simulate the impact a cyberattack 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 asked to identify and discuss the main challenges to increasing awareness of cybersecurity for radioactive sources. They were also asked to discuss necessary competences for individuals in charge of cybersecurity and to draft a hypothetical job description to be used for the recruitment of a new person in charge of cybersecurity for radioactive sources. Their key findings included:

Challenges to raising cybersecurity awareness

- It is difficult to discuss cybersecurity matters in business language.
- Many cybersecurity reports and communication moments already exist, but almost none are directly related to radioactive source security. Too many reports can dilute key messages.
- Many people still do not feel at risk. Some organisations do not feel like they are a target due to their size and/or type of business. If no incident has ever happened, why should they bother?
- It is important to convert high media attention to individual cases.
- A lack of (cyber) security culture exists globally, and many organisations face resistance to change.

Challenges to developing and retaining necessary competences

- A lot of confusion exists between IT skills and cybersecurity skills. They do not mean the same thing, and they require different competencies.
- Developing competencies costs money (both direct costs and staff costs).
- 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 your qualified staff well.
- Perform root cause analysis for problems or unsatisfactory situations. Look at leading companies for models.

WAY FORWARD AND CONCLUSION

As the last activity of the round table, participants were asked to define their personal commitments for enhancing cybersecurity in their organisation/sector and sharing them with other representatives of their stakeholder groups (end users, industry, regulators, international organisations, etc.). Participants were then encouraged to discuss the main findings of the event as a whole group and some of their takeaways and possible follow-up actions.

Examples of these findings include:

- Momentum occurs when 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. The international community is taking the problem seriously. International guidance and training are under development.
- We already have measures in place. A lot of on-going research and development is taking place for defensive security.
- It is more and more common to talk about physical protection 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. Teamwork is encouraged at all levels.
- Resources are starting 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 for enhancing the cybersecurity of radioactive sources. He also committed WINS to building on this success, including regularly updating WINS publications on radiological security to increase guidance on cybersecurity matters and continuing to offer opportunities for information exchange and professional development to all stakeholders who are involved in the security of radioactive sources.

During the evaluation session, 100% of attendees expressed satisfaction with the event and the facilitation process. In addition, 88% 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 also encouraged WINS to ensure a broader diversity of countries attending this type of event.