Proceedings of the INMM & ESARDA Joint Virtual Annual Meeting
August 23-26 & August 30-September 1, 2021

Conducting an online workshop on the supply chain risk in nuclear security: A case study of designing an online event using recorded theatre scene and integrating its findings for professional development.

Masahiro Okuda
Japan Atomic Energy Agency (JAEA)

Lars van Dassen
World Institute for Nuclear Security (WINS)

Bettina Lock
WINS

Naoko Inoue
JAEA

Naoko Noro
JAEA

Yoko Kawakubo
JAEA

Megumi Sekine
JAEA

ABSTRACT

The Integrated Support Center for Nuclear Nonproliferation and Nuclear Security (ISCN) of Japan Atomic Energy Agency (JAEA) and the World Institute for Nuclear Security (WINS) co-hosted a theatre-based workshop on "Supply-chain Risk in Nuclear Security" as an online event for Japanese stakeholders. The proposed paper will feature two key findings: the effectiveness of providing an online activity on nuclear security around filmed theatre scenes and the second one is a case study of awareness raising on supply chain risk in nuclear security in Japan. The first part of the paper will talk through the design process of an online event with the purpose to raise nuclear security awareness. ISCN and WINS have held many "theater-style" events that utilize dramatized scenarios on a hypothetical nuclear security event, and gave participants opportunities to have discussions based on these scenes for almost a decade. Past workshops, which have all been in-person events in Tokyo involved actors playing scenarios on stage. The most recent workshop was the first of its kind to be held as an online event on 16 and 17 February 2021 due to the COVID-19 situation. ISCN requested WINS to duplicate the successful format and create an online version. To accommodate ISCN's needs, WINS most effective options on how to replicate the theatre format, including useful discussion opportunities, and eventually successfully delivered an on-line event designed around recorded theatre scenes and professional facilitation. In respect to awareness raising for supply chain risk in nuclear security, the paper will explain findings formed through the discussion among the participants of the online event. The supply chain risk in the context of nuclear security is a relatively new topic in the nuclear security community in Japan. The paper will examine the importance of identifying supply-chain risks and name possible measures to address supply-chain risk management in nuclear security through the findings from the discussions of the workshop. It will then consider how to use some of these findings to the human resource development activity.

INTRODUCTION

Integrated Support Center for Nuclear Nonproliferation and Nuclear Security of Japan Atomic Energy Agency (ISCN/JAEA)[1] and the World Institute for Nuclear Security (WINS)[2] have held theater-style workshops for Japanese audiences annually since 2012. The theater-style workshop utilizes dramatized hypothetical nuclear security scenarios with simultaneous interpretation at the venue, and participants discuss the topics based

on the contents of the scenarios. Participants are able to think about the situation of the play based on their experiences and perspectives. Such participant's experience is an opportunity for awareness-raising or thinking and beginning to shift perspectives.

In the past, the workshop had been held on the following themes.

- Nuclear security and corporate governance
- Cooperation with external organizations for strengthening nuclear security
- Transparency in nuclear security
- Synergy of nuclear security and nuclear safety
- Insider threats
- Cybersecurity

The workshop themes are defined by ISCN, and WINS develops the scenario based on ISCN's proposal. Domestic nuclear security stakeholders have considerable interests on the recent developments in nuclear security, and ISCN ensure that relevant discussion points are integrated into the workshop.

The workshop on supply chain risk in nuclear security was initially planned to be held in March 2020. However, it was postponed due to the COVID-19 pandemic, and the workshop was transformed into online format and held in February 2021. The workshop sessions were structured around filmed theatre-scenes, plenary and break-out discussions, injects from selected Subject Matter Experts (SMEs), as well as polling questions to support the flow of information.

This paper explains how ISCN and WINS developed the online theater-style events workshop and describes challenges on how to address supply chain risk in nuclear security through the contents of discussion.

THE CURRENT SITUATION IN JAPAN OF SUPPLY CHAIN RISK PERCEPTION IN NUCLEAR SECURITY

Japan addresses nuclear security implementation under the current regulation. Japan's regulation is harmonized with international obligations or guidelines such as IAEA INFCIRC/225/Rev.5. However, the term "Supply Chain" itself is not covered explicitly.

On the other hand, recognition against supply chain risk has gradually increased, especially in cybersecurity.

For example, the government of Japan is developing a national strategy addressing IT systems and services procurement in the context of cybersecurity.[3] The strategy includes supply chain security in the procurement.

The recent cyber-attacks originating in the supply chain also raised concerns in Japan.

PROCESS OF THE ONLINE WORKSHOP DEVELOPMENT AND CONDUCT

With no end in sight for the pandemic, ISCN and WINS started discussions in September 2020 for bringing the workshop online. In response to a request from ISCN, WINS proposed a schedule for a two-day, five-hour workshop that would utilize the theatrical scenario originally developed for March 2020 workshop.

There were two challenges in conducting the workshop online. The first was how to present the play to the participants. In the face-to-face format, the professional actors performed at the venue. The time difference was a problem for the online workshop, as the theatre group AKT Productions[4] was based in London. ISCN and WINS decided to film the plays and add Japanese subtitles.

The second issue was the interaction among the participants in the online discussion. In

the face-to-face workshops, participants was seated at several tables and could discuss in small groups. In this way, it was possible to have more interactive communication among the participants.
About 50 people were expected to participate in the online workshop. The workshop consisted of four scenes, each of them followed by plenary or breakout discussions. It was difficult to achieve the interactive communication as same as face-to-face workshop with online format that just streaming video or delivering presentation.

To solve this challenge, ISCN and WINS decided that two of the discussion sessions following all four scenes are conducted in sub-group.

Minor changes were made to the original scenario to facilitate the filming of the scene and an effective interaction with the participants during the live online sessions.

The online plenary discussions were facilitated by AKT Productions, and ISCN's instructors facilitated the online breakout sessions. During the breakout sessions, participants were divided into five sub-groups, and the group facilitators reported discussion results in plenary. During the workshop, discussion points were suggested by the shared slide or by the polling function of the Zoom meeting.

The event was conducted in English and Japanese languages with simultaneous interpretation.

SUMMARY OF THE WORKSHOP

SURVEY BEFORE STARTING THE DISCUSSION

Before showing Scene 1, two questions were discussed using the polling and the chat functions.

The first one was about participant's affiliation to understand the attributes of the participants. According to polling results, the main represented stakeholders were:

- *Industry and end-users*, such as representatives from nuclear operators like nuclear power plants, fuel fabrication, and research facilities. They are considered as end-users in a supply chain.
- *Vendors and consultants*, such as representatives from companies that provide nuclear security equipment or security services to the end-user. Their business includes repairing and maintaining security equipment. They are suppliers in the supply chain of nuclear security procurement and other services.
- *Education and training organizations*, such as researchers or students who could use small amounts of nuclear materials and radioactive materials for their research. They are also involved in physical protection (PP) as a user of nuclear materials and facilities. They are also end-users in the supply chain.
- *Regulators and other governmental organizations*.

The second part of the survey question was as follows: “I feel confident that my organization has identified and addressed the security risk related to the supply chain.” 55% of the participants agreed or partially agreed with the statement. Amongst those who did not agree with the statement, 20% of them strongly disagreed. It was clear that recognition of the risk and necessary measures against supply chain risk was divided among participants at this moment.

Scene 1

The story of Scene 1 went as follows:

"The junior IT professional, Ana, is having an online discussion with her friend Rosa. Ana reports on her new job but makes a concerned face. She reports having discovered irregularities in her new function while fixing a bug in the company's commercial system which includes sensitive financial information and details of contracts. Rosa questions whether it could be industrial espionage and urges Ana to report it. Ana follows her friend's suggestion and reports her findings to the Chief Nuclear Officer."

Discussion on Scene 1

Following Scene 1, the facilitator invited the participants to identify what they had just observed. A list of key developments was reported - among which was an unauthorized access, a back door, that had been installed in the security management IT system - which seemed to lead to deliberate endangerment of the entire security system. Leakage of sensitive data outside the organization was suspected, and some participants questioned the actions of the security director.

When discussing the question “What does supply chain risk mean to you?”, participants highlighted the challenge of addressing about the supply chain risk, because it is an invisible threat to the nuclear facility and difficult to notice. They also indicated that some people who manage the security systems are not aware of the risk.

Most participants emphasized the importance of the relation between the end-user and subcontractors. In the case of Japan, nuclear facility operation is implemented both by the operator and subcontractors. Subcontractors carry out a wide range of tasks in a nuclear facility—for example, reactor operation, construction, maintenance, administration, and so on. The security of a nuclear facility is also supported by subcontractors such as security measures implemented by civil security guards, supplying and maintenance security devices for the operator.

Especially in supplying security devices, many agents (companies, manufacturers, individuals) are involved. Subcontractors sometimes deal with specialized technology that requires know-how not available at the end-user. Some of the participants pointed out that this problem is similar to insider threat and that the risk of information leakage was one of the possible risks in supply chain.

Finally, participants stressed the need for continuity and stability of supply. The subcontractor's support is necessary to operate the facility. Shortage and other disruptions in the supply chain could put the operation of a facility, including of its security systems, at risk.

Scene 2

As the second session of Day 1, Scene 2 went on as follows.

"Ana has found that Rees Security Systems (RSS), the sub-contractor who installed part of the security system, has given the security department access to information and systems not accessible to the rest of the company. RSS has also been downloading security management data and contract information, as well as communicating security data back to RSS in unencrypted form.

When the Chief Nuclear Officer and the Commercial Director challenged the CEO of RSS, he said he could only discuss matters with the Security Director, who he also said

knew about the alarm monitoring data going back to RSS. He also denied knowing anything about sensitive information being transmitted to his systems."

Discussion on Scene 2

After playing Scene 2, participants were divided into five groups and discussed the following questions:

- What could be the security risks associated with the use of external services? Which security risks arise from equipment or external contractors? and
- How much nuclear security awareness should be expected from external contractors? How do you ensure that external contractors meet your security expectations?

Key findings of the breakout groups included the following:

- Participants were concerned that security awareness among subcontractors is very low. They also highlighted the importance of security awareness of the procurement officer of the end-user who may be involved in screening sub-contractors during procurement. Based on the practices of the participants, security procurement is also led by procurement officers in their organization. It was clear from the discussion that addressing supply chain risk requires the involvement of various stakeholders.
- Various risk mitigation measures were suggested by the participants. They pointed out that education and training are necessary on the subcontractor's side and on the end-user's side. Background checks, trustworthiness, and audits were suggested as other mitigation measures.
- Another finding was around rules and procedures on procurement. A group had suggested a possible problem on checking the related security procurement. Suppose a company is deciding on whether or not to implement checks when procuring security equipment based on the amount of money of the contract, any contracts below that standard would be omitted from the web of checks. It was suggested to consider building new rules and procedures to address supply chain risk.
- Participants finally suggested enhanced information sharing among operators and regulatory authorities.

Based on the discussions that followed Scene 2, participants have discovered possible vulnerabilities and factors that affect to soundness of the supply chain in order to the risk.

Scene 3

Before moving to Scene 3, two SMEs shared their experiences in addressing supply chain risk in nuclear security.

Ms. Carol Higson, Manager in the Security Department at the Urenco Capenhurst Site, made a presentation on supply chain risk management in nuclear security. She highlighted the following three points:

・Ensure any contract includes a security statement.

・Ensure that you have oversight and an intelligent customer for the contract.

・Ensure that the contracting company applies the same vetting and aftercare that you do.

She explained that all stakeholders in a supply chain should have a clear definition and

understanding of their accountability and responsibility. Also, she emphasized the importance of continuous observation and conducting necessary corrective action. According to her, supply chain risk mitigation measures should be conducted during the entire life cycle of the contract.

Mr. Jordan Ross, Supply Chain Director of Bruce Power, was invited to talk about the importance of sharing experiences among nuclear and other sectors, including the financial industry. He suggested the following three points for consideration.

- All organizations are facing similar threats and technology changes, which need to be addressed together across industries. There is a need to share and receive feedback from external stakeholders.
- The intelligent customer is achieved through an organization working together. Ultimately, individuals understand each other's roles, responsibilities, and authorities.
- Where possible, work within existing roles and processes to minimize complexity and transition time when making changes.

After the presentations by SMEs, Scene 3 was played in the following scenario.
"Ana is questioned by the Security Director (SD). SD implies that she hacked into critical national infrastructure IT system by printing a document. Ana defends herself by indicating that she had been asked to do so by the Chief Nuclear Officer. The SD accuses her of being an extremely inexperienced and naïve young woman which Ana immediately pushed back on. Shortly afterwards Ana has an opportunity to talk to the Commercial Director who reassures her that she had done the right thing by reporting the issue. The Commercial Director explains that he does not approve contracts unless their value exceeds a certain threshold and that the security department approves some security contracts directly. It turns out that some of the security contracts had not followed the same procurement policies as other contracts and that sub-contractors had been favored because they had personal relationships with the Security Director."

Discussion on Scene 3

Following Scene 3, the facilitator asked participants, "What have we seen?" and "What does it make you think about?".

Most of the participants pointed out the pre-existing relationship between the SD and the president of RSS. Also, they reported that the contract had been decided by SD without confirmation by other agents in the National Power.

On the other hand, some participants pointed out about a problem in the hypothetical company's posture. As already reported in the discussions after Scene 2, participants indicated that the different procurement policies had been followed and that RSS had been favored in the scene. The fact that the commercial department was not involved in the decision and review of the contract was seen as an institutional problem. Participants also pointed out the lack of security awareness of company management and divisions other than nuclear security.

Following the above discussion, one question was provided to the participant using the polling function of Zoom.

The first polling question was, "I believe my organization's procurement process had effectively integrated security needs." Of all the participants, 7% answered "strongly agree," 55% "partially agree," 34% "partially disagree," and 3% "strongly disagree."

Some participants who agreed with the statement explained that in their company provisions on confidentiality and guarantee against defects are included in their specification document in procurement. Others shared their experiences on their internal procedure to accept a contract.

Another point of discussion was then suggested to the participants by posing the following question:

"What are good practices for effective cooperation between the security department and procurement department?"

The cooperation among the security department and other departments, and the security awareness of other departments had already been addressed in the discussions in the previous scenes. In this discussion, no specific examples of effective cooperation were provided; however, some ideas to address supply chain risk were suggested. For example, one opinion was that the end-user address security threats by themselves through detecting unrightful devices or programs at the time of delivery or while operating the systems. Another participant suggested that the IT department should be involved in computer procurement.

One participant noted that supply chain risk is one of the most unpredictable threats to the nuclear security sector, and that it is becoming increasingly difficult to predict and counter threats in advance, and that it is necessary to think "on the run" about how to do so. That participant also pointed out that it is important to have a culture that does not shy away from changing these methods and rules.

Scene 4

Scene 4 was the final part of the workshop. The scenario proceeded as follows.

"The Commercial Director of NationalPower has a rather uncomfortable meeting with the Director of Regulation at the Office of the Nuclear Safety and Security Regulatory Authority. The security breach is now in the news and NationalPower has told the Director of Regulation that their response was to conduct an internal enquiry. They say it has never been their policy to involve the regulator with commercial matters, even though they have now discovered irregularities in procurement going back five years. Reliability issues were pointed out to the Security Director who gave the Regulator assurances that they were just random faults, and the Commercial Director asks why those reports were not circulated to other senior managers. The Director of Regulation says that NationalPower are in breach of their license to operate as they clearly have not shown due diligence in their dealings with their supplier. The Commercial Director disagrees, but the Director of Regulation makes it clear that her office views the matter so seriously that they will be pursuing a legal course of action."

Discussion on Scene 4

After playing Scene 4, a breakout group discussion was conducted with the following discussion points:

- "At what point is equipment checked against specifications before installation?" and "Who checks it - the supplier, the customer, or an independent body?"
- Following the invited SMEs' inject on regulatory matters, what is the Japanese approach to regulating the supply chain? How do you demonstrate that you have taken necessary measures for the supply chain?

Key findings include the following:

Equipment should be checked at the time of installation. However, in the case of procurement of more important goods for facility operation and security, the manufacturing process should also be checked. Some argued that it was important for end-users and suppliers to mutually determine who will check the equipment. Some of the participants indicated that based on their experience there are no third parties checking the equipment. It was finally mentioned that industrial standards, such as ISO certification, could be useful in determining and confirming the specifications.

CONCLUSIONS

According to the post-workshop survey, all respondents answered either “very much satisfied” or “satisfied.”

The online theatre-based format for the workshop through the Zoom platform was successful and will be considered again in future.

Supply chain risk was a relatively new issue for many participants, and the workshop itself was a novel topic in Japan as it brought this issue into the nuclear security field. However, as the polling result in Scene 1 suggested, the stakeholders in Japan already applied measures to deal with the supply chain risk in general, such as rules in the specifications and audit.

On the other hand, there are some new findings for the participants. According to the post-workshop survey, some participants wished their procurement staff could have participated in the workshop. It was an opportunity to discover the involvement of new stakeholders in dealing with emerging security risks.

This workshop was the first online ISCN-WINS workshops that have been held so far. One of the challenges was that there was less interactions among participants than in the face-to-face workshop. Among the arguments made by the participants during the workshop, many controversial points remained, such as the each roles and responsibility of end-users and suppliers in ensuring the appropriateness of procured equipment.

This supply chain issue is likely to remain an important topic in the future. In this context, it is necessary to provide more opportunities for discussion in the field of nuclear security.

ACKNOWLEDGEMENTS

The authors would like to thank the participants of this workshop for their active participation which made the workshop successful.

We would also like to extend our gratitude to Mr. Pierre Legoux and other WINS staffs for their efforts in organizing the workshop, as well as Mr. Roger Howsley, former executive director who was involved in the initial scenario development phase.

We would like to thank Mr. Marc Bolton for his excellent facilitation and AKT Productions for creating a wonderful dramatized movie to prompt the participants' thinking.

Ms. Carol Higson and Mr. Jordan Ross shared their meaningful experiences and perspectives as SME.

Finally, we would also like to thank our ISCN technical support team, especially Ms. Rieko Sugiyama, Ms. Risa Motokawa, Ms. Junko Ashima, Ms. Takako Uchikoshi and Mr. Nobuhiko Hasegawa for their efforts in the operation.

[1] Tokai, Ibaraki, Japan.
https://www.jaea.go.jp/04/iscn/index_en.html

[2] Vienna, Austria.
https://www.wins.org/

[3] "Outline of Japan's next Cybersecurity Strategy, which will come out by the end of this year." 8 July 2021, National Center of Incident Readiness and Strategy for Cybersecurity.
https://www.nisc.go.jp/eng/pdf/txt_next_CS_strategy_outline.pdf

[4] London, U.K.
https://www.aktproductions.co.uk/