The Effects of COVID-19 on Radiological Security – Insights from Radioactive Material Licensees

D. Higgins
Pacific Northwest National Laboratory

T. Roush
Pacific Northwest National Laboratory

J. Carneau
Pacific Northwest National Laboratory

K. Charbonneau
Yale University

ABSTRACT

As the world continues to suffer the effects of the COVID-19 pandemic, organizations, including those possessing high activity radioactive materials, are struggling with continuing daily operations given the challenging conditions the virus has created. The pandemic has stressed organizational resources to the limit and leaders of these organizations are faced with challenges on multiple fronts, including maintaining the integrity of their radiological security plans. Although many of these organizations have emergency plans or disaster recovery capabilities, few were able to anticipate the prolonged, far-reaching consequences of the pandemic. Radiological assets serve important roles in medical, research, and commercial applications. However, if these radioactive materials fall into the wrong hands, they could be used in a radiological dispersal device ("dirty bomb") or in other acts of terrorism. The U.S. Department of Energy's (DOE) Office of Radiological Security (ORS) partners with organizations to improve the security of their sensitive radiological assets. These partnerships have given ORS a unique perspective on the effects of COVID-19 as it relates to the security of radioactive materials. The authors of this paper interviewed sixteen U.S. radioactive material licensees, security integrators, and other industry stakeholders to gain an understanding of the "new normal" as it relates to radiological security. This paper will explore the effects of the COVID-19 pandemic on the security of radiological assets, highlight common issues, and offer suggestions for addressing security concerns during these challenging times. Furthermore, this paper will identify lessons learned from the pandemic that can be applied to improve radiological security plans.

INTRODUCTION

What started as a novel coronavirus outbreak in Wuhan, China, in late December 2019, has transformed into the worst global pandemic of the last 100 years. As of the writing of this paper, the world continues to be impacted by the COVID-19 pandemic. Interestingly, many institutions involved in the fight against COVID-19, such as hospitals and pharmaceutical companies, also possess significant quantities of radioactive materials. The threat of a bad actor using radioactive materials in an act of terrorism is always present, but how a pandemic could affect probability or

consequences of this threat is unknown. This paper will deliver insights directly from those managing the security of radioactive materials during the pandemic.

DOE's National Nuclear Security Administration's ORS mission is to enhance global security by preventing high activity radioactive materials from being used in acts of terrorism (Security, 2021). Put simply, ORS partners with organizations to reduce the risk radioactive materials pose. From this point forward, radioactive material licensees who have formally partnered with ORS to improve the radiological security of their materials, will be referred to as "partner sites" (which is a smaller population of radioactive material licensees). Many partner sites, such as hospitals and pharmaceutical companies, are also on the front lines of fighting COVID-19.

The topic of the pandemic's effect on radiological security is not completely novel. Security professionals, including those within ORS, have questioned how the pandemic has affected partner sites. However, the authors of this paper informed such perspective by interviewing U.S. radioactive material licensees. These interviews were conducted virtually due to the policies and procedures implemented in response to the pandemic. Interviewees from partner sites were fulfilling a variety of roles for their organizations. The most common roles of those interviewed were radiation safety officer (RSO) and security director. Sixteen interviews were conducted with partner sites in the first half of 2021. Additional interviews were conducted with a security vendor and a response personnel representative (local law enforcement) who regularly engage with radioactive material licensees.

It is also important to note the limitations of the virtual interviews conducted. Most interviews were conducted with staff generally considered to be management personnel. It is possible their perspective may be focused on their management responsibilities versus the day-to-day operations of one or more assets in question. Furthermore, many interviewees have been working remotely (off-site) during the pandemic. Even though interviews were conducted in confidence, it is possible that interviewees may still be reluctant to share information that paints their institutions in a negative light. The authors also did not have the opportunity to observe the conditions at the radiological facilities represented in this paper. Lastly, even though the worst of the pandemic appears to be over in the U.S., it is possible the full scope of the pandemic's effects are not fully realized as of the writing of this paper.

The conversations with partner sites were organized using the recently released World Institute for Nuclear Security (WINS), "Methodology for Assessing the Effectiveness of Security Arrangements at Gamma Irradiation Facilities" (World Institute for Nuclear Security, 2021). Even though the framework is intended to serve as a methodology for a specific type of facility, it lends itself well to providing a framework for assessing security at all facilities containing radioactive materials. Not all areas were covered, and some were modified to broaden or narrow the topic. The remainder of this paper uses this methodology to organize the effects of the pandemic, document partner site best practices, and draw conclusions that could apply to other radioactive material licensees. This includes both ORS and non-ORS partners, heretofore referred to as "licensees."

Governance Arrangements

The pandemic has forced partner sites to reconsider the management of their radiological devices. The management of radiological assets requires the coordination of multiple levels of the organization (from temporary project hires to the leadership team) as well as multiple functions (safety, security, facilities, risk management, and others). No two institutions manage these assets in quite the same way and the pandemic tested these arrangements.

Security Plan

With few exceptions ("normal" adjustments that would have occurred regardless of the pandemic), partner sites have not altered their Nuclear Regulatory Commission (NRC)/Agreement State Security Plans as a result of the pandemic. Sites commented they were able to execute their existing plans regardless of the operational impacts or new working environment. This is because many RSOs were deemed to be essential workers along with their associated on-site security forces. When stay at home orders were issued across the U.S. in the spring of 2020, several partners mentioned they looked into altering their security plans to account for any operational changes but were reassured that their response forces still maintained pre-pandemic capabilities.

Security and Risk Prioritization

Overall, partner sites prioritized security similarly during the pandemic. In many cases, the role of on-site security personnel was expanded to include health screenings, entry point monitoring, and other pandemic-related roles. Security department headcounts increased in several cases due to these additional responsibilities and the need for a "bench," if personnel were unavailable due to quarantines or caring for sick family members. Every partner site restricted access to their campuses in some capacity, most commonly by restricting public access buildings with electronic access control systems and requiring certain credentials to enter the facility.

General perceptions about the national security threat that radioactive materials pose remain mostly unchanged. In some instances, partners were concerned that periods of limited operations might create a window of opportunity for theft or device tampering. These sites responded by either increasing patrols of areas housing materials of concern or were being especially vigilant about frequently assessing these areas remotely (via the video management system).

Budgets

Generally, for profit partner sites have not been drastically affected financially by the pandemic. When discussing the topic of budgets with universities, the response was mixed. While there seemed to be consensus that discretionary spending had been limited, some were able to absorb and redirect resources easier than others to cover any additional costs resulting from their institutional response to the pandemic. Public universities were in some cases subject to local and state budget reductions, where private universities were able to remain more flexible in budgetary spending. It was also communicated in some instances that security department budget allocations were increased to account for the increase in staff overtime and additional hiring needed to fulfill the additional duties brought on by the pandemic.

Financially speaking, the pandemic has most greatly impacted hospitals and medical centers as more profitable procedures, such as elective surgeries, were put on hold. As a result, hospitals had to make difficult decisions to freeze staff pay and hiring and, in more rare occurrences, furlough non-essential resources. One licensee remarked that COVID-19 has created the worst financial environment in their 50+ year career. It was commonly communicated that capital projects had been put on hold or were subject to drastic budgetary cuts. While these new financial burdens affected radiological security indirectly at times, the more direct impacts were minor. Partner sites were still confident security would not be impacted in the short term. At the time of publishing, elective surgeries were being performed and hospitals were optimistic their financial situation was recovering. Licensees should prioritize security budgets during any period of financial hardships and avoid classifying it as simply another overhead expense.

Source Disposition

Any organization wanting a permanent solution to eliminating the risk that comes with managing radioactive materials should take steps to identify a way to transition to non-radioisotopic technologies. Many licensees have dispositioned some or all of their radiological devices through ORS. Unfortunately, but not surprisingly, the pandemic negatively affected the process for radiological source dispositions. Those with plans for source disposition before the pandemic are now faced with recovery delays due to pandemic-related travel restrictions. Additionally, partner sites that were purchasing non-radioisotopic devices or funding source removals themselves, found some projects put on hold due to restrictions placed on capital expenditures. One partner site remarked that the pandemic helped the organization realize they could accomplish all of their research with one device and could dispose of the others. Licensees should continue to evaluate their needs for radioactive materials as well as their ability to transition to alternative technologies on a periodic basis, as non-radioisotopic devices continue to evolve both in terms of reliability and enhanced capabilities.

Physical Protection

For partner sites typically open to the public, such as hospitals and universities, the pandemic has caused site management to limit the number of non-essential personnel allowed on-site. Most hospitals interviewed have limited access to their facility to patients (or in some cases, patients with one caregiver). This has created an environment where many hospitals are relatively full in terms of their hospital bed census, but, according to interviewees, their hospitals feel less busy and there are fewer disturbances requiring a response by security.

The pandemic has resulted in partner sites implementing and maintaining strict social- and physical-distancing protocols within their facilities. As a result, some partner sites stationed security personnel at entry points of the facility to perform symptom checks and also to maintain a count of the number of personnel inside the facility. This new practice has resulted in interviewees having an increased peace of mind that only authorized individuals are within their facilities. This practice or something similar in nature, could be used by licensees as an additional security measure when maintaining a heightened security posture.

Sometimes the combination of reduced staff and automatic software or firmware updates can also create issues. One interviewee commented that a Microsoft Windows update caused a network video recorder (NVR) to cease functioning. The facility was unaware of this issue for at least three days and the issue was not able to be resolved immediately due to minimal staff on-site. A best practice would be to confirm the functionality of all systems after any updates are scheduled to take place.

All site partners commented that their service agreements for their physical protection systems remained active. Service visits may have been delayed, but none were missed. This assertion was contradicted by a security vendor interviewed who was aware of at least one service agreement having lapsed. Whether serviced by an external vendor or by a licensees' own staff, it is critical to continue to test, maintain (including software and firmware updates), and repair physical protection systems in a timely manner.

Several partner sites commented on the lack of availability of physical protection system components. Sites were told by their vendors that the pandemic had created supply chain disruptions and delays. Vendors typically do not maintain a stock of spare equipment for all security equipment a partner site may need. If necessary, partner sites may replace non-functional security equipment supporting radioactive materials with equipment that may be protecting lower priority assets. Licensees should also consider stocking critical spare equipment that is unique or specialized.

Interestingly, one benefit of the pandemic is it has forced greater coordination of various functional groups within partner sites. Radiation safety, security, facilities, safety, human resources, and other functional organizations were required to form integrated teams and establish pandemic policies and protocols for access to their radiological assets. Once established, these groups continued to cooperate to assure staff were "cleared" by all required parties. For example, human resources might have to confirm that a daily health check was completed, safety might have to verify the number of personnel scheduled to be in a research laboratory, security might have to reactivate an access control credential, and radiation safety might have to confirm unescorted access is allowed. Several sites remarked that additional coordination was a good thing, and in some cases led to greater interconnectedness of functional data systems. The ability for organizations to quickly and effectively establish multidisciplinary teams to respond to unique problems or crises, such as the pandemic, is a valuable one. Such an ability would likely prove invaluable for the coordination of a response to an emergency involving radioactive materials.

Response

Several hospitals noted that on-site security has had their role expanded. For example, some hospitals had to dedicate more time to enforcing strict visitor policies. Several interviewees noted hospital visitors have become more combative, possibly due to the stresses the pandemic has put on the public. In some cases, overtime work became mandatory for on-site security due to staffing shortages. An additional complicating factor was unexpected retirements, some citing personal health and safety concerns.

Relationship with Response Entities

Many partner sites have invested years in their relationships with local law enforcement agencies. Several sites commented these investments have been advantageous as law enforcement continues to prioritize their sites throughout the evolution of the pandemic. No partner sites thought response times had increased as a result of the pandemic. These statements were typically qualified with the thought that it is possible response times slightly increased during the strictest mitigation measures (e.g., stay-at-home orders). Response entities are often hesitant to admit to any reduction in capabilities. However, partner sites provided a few examples of false alarms where the response was similar to a pre-pandemic response.

Training (Response)

Training for response agencies was temporarily put on hold during the pandemic. This hold was especially true for coordination of in-person training activities, such as physical walkdowns of facilities (likely due to social and physical distancing concerns). All partner sites intend to resume training and coordination with response agencies as restrictions from the pandemic are eased. All licensees should resume response training as soon as it is feasible to do so and consider initiating a response exercise (such as a tabletop exercise) to return response coordination to pre-pandemic levels.

Security Awareness and Culture

Even though partner sites did not have to change their formal security plans, the specifics of how users gain access to their radiological devices changed during the pandemic. Interviewees commented that users were generally understanding of the new safety and security requirements and there was mostly compliance with the new protocols. There were a few examples provided of staff not displaying new badges (which signified unescorted access to radioactive materials), wearing facemasks, completing health screenings, or other violations of protocols. Partner site management was typically able to address these violations with training or simple reminders.

Security Culture

Facemasks are useful for preventing the spread of COVID-19, but widespread mask usage, especially at partner sites, has created an environment where staffs are focused more on assuring mask usage and less upon who is accessing their facilities. One interviewee commented that front line staff were being required to review visitor COVID-19 questionnaires, perform temperature checks, and enforce mask requirements. Due to the completion of these duties, identification or badge checks were commonly missed or hurried. Once in the facility, non-security staff were unlikely to challenge visitors to the facility who were wearing masks. Several interviewees remarked that situational awareness has diminished at facilities due not only to facemask policies, but also to the low staffing levels sites are maintaining during the pandemic.

Several partner sites commented that a component of their security arrangements were practices encouraging the reporting of suspicious behavior: a “see something, say something” policy. With fewer staff on-site and security personnel handling other duties, there were fewer opportunities for someone to “see something” and situational awareness has likely decreased among partner

sites. A possible alternative may be to increase the assessment of video management systems or security patrols for sensitive areas. One positive example of a strong security culture was during times of reduced on-site security staffing, security managers opted to pull security off of ancillary building postings so that buildings with radioactive materials would be staffed at pre-pandemic levels. Licensees may also need to consider adjusting their strategy for maintaining and promoting a strong security cultures given the increase of staff working remotely.

Training (Site Personnel)

Overall, required training was still conducted, most often via a virtual platform or in-person with social distancing. Training that was not driven by regulations or other safety-related concerns (such as awareness or familiarization-type training) was delayed in some cases.

Cybersecurity

It was unanimously agreed upon by partner sites that cybersecurity threats continue to persist. The feeling among RSOs is that the threat was especially difficult to mitigate in their roles because they must place a significant amount of trust in IT personnel and security vendors to maintain security systems appropriately. In some cases, IT personnel made proactive cybersecurity-related policy changes (e.g. removal of user permissions) that may have increased overall security, but unintentionally inhibited operations. High-profile cyber breeches and ransomware attacks continued to weigh heavily on the minds of partner sites. Even though it is not a novel concept, licensees should continue (or, worst case, initiate) cybersecurity programs. User training should include tangible actions that increase user awareness of such attacks and how to identify how each staff member can take an active role in supporting such a program. Management must clearly communicate expectations to staff members and promote a feeling of shared responsibility for protecting an organization's sensitive data.

With the quick transition to a virtual work environment (in March of 2020 for many organizations), many physical devices went from the relative physical safety of corporate offices to apartments, homes, and in some cases, vacation properties across the world, making them generally less physically secure. To make matters more challenging, most devices went from primarily residing on the relative security of corporately managed networks to communicating across a multitude of smaller networks, mostly managed by individuals. There are several actions licensees can take to mitigate the threat posed by this new environment. Management should review the overall attack surface, attack paths, and attack vectors to assure they understand when and where systems are most vulnerable. Considering the complexity added due to the increase in remote work, it is vital to identify and implement robust endpoint security. It is also important for management to understand the interconnectivities between various systems and security zones. Lastly, management should honestly assess the organization's overall cybersecurity hygiene, culture, and awareness level, and look to improve upon its posture whenever possible.

Information Security

Sensitive information pertaining to radioactive materials (e.g., security plans) was reported to be protected at similar, pre-pandemic levels. Many partners have developed secure shared drives or

other means of protecting this data, which provided a consistent level of security during the pandemic. This typically included password protection, encryption of data, and limited distribution. There was at least one example of sensitive information being left on a desk, likely due to the quick shift from on-site to remote work locations. Regardless of the state of the pandemic, licensees should continue to promote effective "OPSEC" (operational security), denying an adversary or potential adversary any information that might be useful to them.

Personnel Security

The pandemic created a difficult environment for managing a productive, safe, and secure workforce. Partner sites focused on retaining employees and were typically successful in doing so despite the financial hardships mentioned earlier. In many cases, partner sites were attempting to hire security staff. The demand for hiring was driven by the increased role of security staff in COVID-19 safety protocols as well as decreased availability of current security staff due to personal sickness, required quarantines, care of family members, etc. Several partner sites were hiring additional research staff to support the development and production of COVID-19 vaccines and therapies.

Vetting

The availability of fingerprinting and background checks did appear to be limited, especially during the worst of the pandemic. The typical fingerprinting process requires individuals to be physically close to one another, and these activities were limited or put on hold. Further compounding the issue, was that fingerprinting is often completed by local law enforcement and, given their strategy of minimizing physical contact with others during the pandemic, many police stations were closed to the public. Partner sites often relied upon the escorting of individuals who were unable to be fully vetted during the pandemic. Although not a substitute for fingerprinting and background checks, informal interviews, and check-ins from line managers to see how staff are coping with the pandemic may help to mitigate some of the effects of standard vetting processes not being available. Additionally, as new staff are brought into licensee organizations, especially those staff in positions with access to sensitive information or radioactive materials, it is critical they are properly vetted to mitigate the insider threat.

Insider Threat

It is no secret the pandemic has placed added stressors on families world-wide. The way in which an organization adapted to the new realities the pandemic imposed, could make a significant impact in either increasing or reducing the insider threat. By definition, an insider is someone who "takes advantage of their access to do harm to the organization's mission, products, resources, personnel, facilities, information, equipment, network, or systems" (Insider Threat Mitigation Guide, 2020). Per one RSO, the insider threat is still the most likely scenario for a radiological security incident. While several interviewees continued to reiterate that the insider threat is "very real," there is still a lack of formal insider threat programs being implemented at some institutions. The potential for decreased morale in the workplace due to increased isolation and additional burdens placed on individuals and families only stresses the importance of mitigating the insider threat by implementing and maintaining a separation of

duties with access control and monitoring capabilities. Sensitive information is exposed to less risk when there are mitigations in place for access control and alarm adjudication. Simple strategies such as separation of duties (e.g., a person with unescorted physical access does not have access to the video management system [assessment capability]) also have a role to play.

Insiders, including those under stressful situations, can still introduce risk to security without intending to do so. They are known as unwitting insider(s). A simple careless act such as misplacing a badge, opening a suspicious email, or discussing sensitive information in a public setting could be a mistake that is part of a larger security incident. That is why it is important to build in systems to mitigate the risk posed by insiders or, more accurately, the risk posed by the human element. This is especially important during a period of unprecedented stress when individuals are more prone to making mistakes that an adversary could exploit.

Organizations wanting to actively combat the insider threat might consider the inclusion of; employee assistance programs, mental health awareness campaigns, a process for anonymous reporting of suspicious behavior, physical security components intended to detect and deter insider threats, and a formalized insider threat mitigation program. Staff training also plays a large role in mitigating the insider threat. Any staff member responsible for the security of radioactive materials and the safety of their staff, should be trained to recognize suspicious behaviors and how to mitigate potential threats. This could be much more challenging to assess given how intermittent telework and virtual engagements replaced prolonged in-person interactions. It is important that licensees recognize these new challenges brought about by the pandemic and do not discount the value of a formal insider threat mitigation program.

CONCLUSION

In conclusion, partner sites have demonstrated resiliency and adaptability in the face of the pandemic. The pandemic has challenged partner sites in ways few could have anticipated. In response, partner sites developed new policies and practices to assure their radiological devices remain as secure as they were before the pandemic.

Conclusion 1: Sites' overall success in dealing with the pandemic from a radiological security perspective is largely due to factors that existed before the pandemic.

Nearly every partner site expressed their need to continue to meet their NRC or Agreement State regulations despite the pandemic. This statutory requirement empowered RSOs and security managers to navigate their organization hierarchies to adjust quickly to the new environment. Audited site security plans had been established and provided a good baseline from which to build alternative security arrangements for the radiological devices. The ability for staff (especially staff in radiation safety) to work remotely allowed for continued oversight and management from the safety of their own homes. Technology was used to augment or partially replace personnel. Lastly, many partner sites have established strong working relationships with local law enforcement agencies. As the pandemic unfolded, partner sites and these agencies were able to coordinate and mitigate some of the risks associated with the changing working environment.

Conclusion 2: Limiting access to site facilities has security benefits beyond minimizing the transmission of COVID-19.

The reduction of non-essential personnel, staff, and visitors from partner sites has eased some of the burden placed on on-site security forces. There is better awareness for whom is on campus and better control of protected areas. Suspicious behavior stands out and unauthorized individuals are easier to identify and confront. Most partner sites intend to continue the limitation of access to certain buildings or parts of buildings. As the pandemic restrictions ease, the continued policy of limiting access to campuses must be balanced with institutional values of efficiency, openness, and collaboration.

Conclusion 3: The threat posed by insiders continues to persist. Sites should remain vigilant and establish (or continue) an effective insider threat mitigation program.

The pandemic has stressed organizations in many different ways. What may be overlooked is how the pandemic has stressed individuals within each organization. Individuals have dealt with personal or family health issues, financial hardships, changes in childcare arrangements, new work environments, reduced social interaction, and other stressors. Any of these challenges could have a profound effect on the physical, mental, or emotional wellbeing of employees and could increase the risk of an insider threat, whether intentionally or not. Licensees should incorporate the insider threat mitigation strategies previously mentioned into all elements of security arrangements.

ACKNOWLEDGMENTS

The authors express their appreciation to the leadership at ORS for their support and sponsorship of this effort. The authors would also like to thank the interviewees that took the time to participate in the interviews.

REFERENCES

Security, T. O. (2021, June 23). *ORS Portal*. Retrieved from ORS Portal Home Page: https://orsportal.org/en/home

Methodology for Assessing the Effectiveness of Security Arrangements at Gamma Irradiation Facilities. World Institute for Nuclear Security. (2021, April 23). https://wins.org/document/methodology-for-assessing-the-effectiveness-of-security-arrangements-at-gamma-irradiation-facilities/

Cyber Security Best Practices for Users of Radioactive Sources. Office of Radiological Security. (2018, January).

Insider Threat Mitigation Guide. Cybersecurity and Infrastructure Security Agency. (2020, November). https://www.cisa.gov/sites/default/files/publications/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf