Proceedings of the International Symposium on the Packaging and Transportation of Radioactive Materials PATRAM 2019
August 4-9, 2019, New Orleans, LA

DOMESTIC RADIOLOGICAL TRANSPORT SECURITY RESPONSE ENHANCEMENT ANALYSIS*

Ken Martin
Oak Ridge National Laboratory
Oak Ridge, TN

Commie Byrum
Oak Ridge National Laboratory
Oak Ridge, TN

ABSTRACT

Response to an event involving radiological security can be complex and challenging for law enforcement and other responders, especially in cases of radiological transportation theft or sabotage. During routine events, response to an incident by law enforcement will typically occur rapidly and be short in duration. In contrast, a long-term incident involving multiple responding agencies to a rarely occurring event can pose additional challenges that must be addressed. While response strategies may be in place, the infrequency of the event makes it difficult for responders to know that those strategies will be effective, assuming a strategy to address a radiological theft or sabotage scenario is in place. To ensure radiological security, enhanced security measures and strategies in responding to a radiological transportation theft or sabotage event are recommended.

INTRODUCTION

With the large number of Category 1 and Category 2 shipments of radiological material on the roads today, timely response by law enforcement during an attempted theft or sabotage scenario is critical. To enhance this response, Oak Ridge National Laboratory has examined and proposed techniques to improve the response of law enforcement by incorporating physical security features of conveyances and implementing administrative practices to include policy development and training in the field.

The results of the analysis yielded two focus areas: (1) enhancing physical security systems of the conveyance and (2) policy and training.

1. PHYSICAL SECURITY SYSTEMS ENHANCEMENT

The security features that are provided for radiological shipments are intended to restrict unauthorized access to the radiological sources; however, many of the security features were designed prior to concerns about radiological dispersion devices. These features provide a

minimum amount of protection and safety features, but they may not be entirely effective against a determined and knowledgeable adversary (Gitomer et al., 2003). Nevertheless, anything that deters one from removing a source can provide a measure of protection and reduce concern, but there are areas for improvement.

One way to address the threat to these shipments is to enhance the physical security systems (PSS) of the conveyance. By applying multiple PPS layers, one can start to mitigate the risks posed by the adversary team and gain valuable time for the responders to arrive to the scene. One area that can greatly aid in this is by applying new technologies where applicable. New technologies and administrative procedures should be integrated to create a complete system capable of detecting and delaying the adversary. The goal is to add resiliency by hardening systems using redundancy and robustness.

1.1 DETECTION

Detection is the first key function used to prevent an adversary from accomplishing a malicious act. For a response to a theft or sabotage event to be effective, the malicious act must be known immediately. The earlier an adversary is detected, the greater the chance that the response force will be successful in preventing the act (US NRC, 2014). The detection elements are least effective when they are not supplemented by operational and procedural controls, maintained, tested, or correctly installed. These lapses in the implementation of detection elements can lead to a single point failure in a security system. Security systems with single point failures are particularly vulnerable to insider exploitation because an insider may know more about the facility, in this case the conveyance, and its detection capabilities than most security managers. Unfortunately, not many detection elements are built into systems on the conveyances. The shipments greatly depend on the driver(s) and the GPS system for detection, and both the driver(s) and the GPS can be easily defeated. Additionally, people generally do not perform well at detecting threats. A common mistake is to assume that personnel will be able to detect a threat in an enough time to respond or at least start the response to an event (Concentric Security, 2009).

1.1.1 Immediate Detection

One of the first areas to address is immediate detection that a theft or sabotage attempt is occurring. This detection relies primarily on the drivers, escorts, or, to a limited degree, the GPS system. However, other sensors should be integrated on the conveyance to alert a driver or a tracking center that an event is occurring. Monitoring items such as hard braking, swerving, and tire pressure could also be used as indicators. The use of cameras on the conveyance should be considered and could be placed in the cab, so that a monitoring station knows who has control of the vehicle, or in the cargo area, so that the material is under surveillance. In addition, sensors could be added to the trailers or cargo area that contains the material. Furthermore, these systems must be complemented with administrative controls such as adequate training, performance testing, two-person rule, and strict access control requirements.

1.1.2 Assessment

If the physical security system receives an alarm, an accurate assessment is needed to start the response. Without this assessment, a response is nonexistent. One area for improvement is ensuring that the drivers of the conveyances know what constitutes a threat. Drivers serve as the first line of defense, so it is imperative for them to be aware of the best practices when it comes to identifying risks and threats. This can be addressed by training and awareness programs. This training would not only include what danger signs to look for but also what information is important to report so that the dispatcher/911 center can get this information relayed to the responders.

1.1.3 Communication

An important component of response is communication or the dispatch to an event. Ensuring that information concerning the event is dispatched quickly and prioritized according is critical. Ensuring that the attack is given appropriate priority over other calls will be one of the factors that will determine if neutralization of the threat is achieved. A large part of this notification is not only starting the initial response but also the follow-on actions and agencies that will be needed for this type of event. Interviews from law enforcement personnel indicated that 911 dispatchers need additional training on responding to radiological transportation emergencies. A 911 dispatcher who receives a call regarding the theft of a radiological shipment could very easily handle it like any other stolen vehicle, as he or she may not fully understand the vulnerabilities associated with these types of shipment. This lack of knowledge could lead to critical response time being lost.

Perhaps the most effective way to enhance the response portion of the PSS system is to ensure that the dispatchers understand the danger of these shipments. This could be accomplished through awareness and training for the dispatchers. Also, the role of dispatchers must be recognized as generally the first member of the responder community to become engaged in the event and thus must become part of a seamless response. One way to assist in this area is to create a “Dispatch 101 for Radiological Theft and Sabotage Events” and field training educational program. Also, it is beneficial to integrate dispatch into all aspects of training and exercise scenarios.

1.2 DELAY

Delay is a critical component of any physical protection system. An effective delay system should consist of multiple types of delay mechanisms designed to hamper the adversary team and assist the response forces. The delay elements are most effective when used in conjunction with detection elements against attacks by outsiders and less knowledgeable insiders. Insiders with the necessary access authorization and knowledge of the overall security system may be able to defeat all delays before the response force can arrive. The detection must precede delay for the delay to truly be effective. Delay mechanisms should be numerous and increase in sophistication as the adversary moves closer to the target, with each additional barrier requiring additional tools and/or access authorizations.

In a traditional system, delay elements are placed in conjunction or with detection elements, but with the conveyances used in the radiological industry, the elements are at times separated (i.e., when the driver is on a break). This greatly benefits a malicious insider because it allows him/her a window of opportunity to exploit the system. Once an adversary team has control over the conveyance, there are no real barriers to either taking the conveyance or gaining access to the container. Delay elements consist of the disablement of the conveyance and some trailers and the material container.

1.2.1 Conveyance Delay

Delay is the one aspect of the system where the most benefit may be gained. To enhance delay, the conveyance must first be taken away from the adversary. This is done by disabling the conveyance, trailer, or both. The major weakness of a disablement system is that one of the drivers must activate the disablement system. If the driver is an insider, the system is simple to defeat by simply not activating it. Current conveyances have a built-in disablement technology, but it would be beneficial to evaluate the use of remote disablement. Remote disabling systems can also be integrated into a remote panic or emergency notification system. In addition, during an event, a driver can send an emergency alert by pressing a panic button. This would allow the conveyance to be remotely alerted and to allow a dispatcher to evaluate the situation, communicate with the driver, potentially disable the vehicle, and start a response if needed.

1.2.2 Security Container Delay

Second, we must force the adversary to remove the material from the container. This can be achieved by disabling the conveyance. Once the conveyance has been disabled, the adversary is forced to remove the material from the conveyance. We achieve some delay time from the material container, but the delay time varies greatly depending on the container that is used, and the containers are built primarily with safety in mind. Many of these containers require special tools to gain access, but this can be overcome with the use of explosives or other types of tools such as torches. There are no other significant delay barriers that impede the adversary from accessing the material. To address this issue, containers in the future should be built not only with safety in mind but also with security as a consideration. Finally, additional delay measures to be built around the shipping container should be examined for feasibility.

1.3 RESPONSE

Response to a radiological theft or sabotage event is a concern because of the excessive amount of time it can take for the responders to find the conveyance and then neutralize the threat. For a response to be effective, both interruption and neutralization of the threat before the adversary can complete their task are required (Sandia National Laboratories, 2018). In addition, response must be of adequate size and arrive in a timely manner and have the proper response protocols in place. These response plans and procedures need to be well documented and validated. To be effective, response force deployment is dependent on the detection of insider actions and the communication that an event happening or assessment of the activity. The average response time of law enforcement in the United States is 18 minutes (National Sheriffs' Association, 2016). This time

can be even longer if it takes up to 2 to 4 hours to notify local authorities that a shipment has been lost. This delayed response time gives the adversary more time to take the material or create a potential radiological dispersal device. The insiders can significantly extend this time, depending on his or her actions or inaction at the scene.

Compounding this problem is a gap in training for law enforcement. A recent review of training for law enforcement showed that little training is available on conducting a response to a theft or sabotage event of radiological material. Law enforcement will be the primary responders to an event involving an attack on a radiological shipment. In their position on the front lines, their work arguably has the most significant impact regarding response and overall system effectiveness. This lack of training could affect response times significantly due to the uncertainty on how to respond. Interviews with local and state law enforcement officers indicated that training in this area is either extremely rare to nonexistent, or it has been more than 10 years since any training has been conducted.

2. ENABLEMENT

To enable law enforcement to be able to effectively respond to a theft or sabotage scenario, there needs to be a focus on building the strategies, tactics, organizational structures, processes, partnerships, and tools. This can be accomplished by ensuring that response organizations have sound and effective policies already in place. In addition, these policies need to be examined and tested to ensure they are effective and meet their intended objectives.

2.1 POLICY

An effective response to an attack on a radiological shipment will be greatly based on the advance work agencies perform in the areas of policy, planning, training, and exercises prior to an event. Because of the complexity of such an incident, the importance of coordinated pre-event work is crucial. Formalizing responsibilities and processes through sound policies and practicing them both within agencies and among outside agencies before an incident occurs helps establish and maintain the relationships needed to effectively respond to a theft or sabotage event. For this reason, agencies and partners need to be knowledgeable of and ready to implement best practices for an effective response to an attack on one of these shipments.

The development of policies and procedures responding to a theft or sabotage event will guide the initial and coordinated response of law enforcement and others as appropriate for the recapture of stolen Category 1 or Category 2 controlled radiological material. Lessons learned have shown the value of pre-operational response planning by agency subject matter experts that includes a response strategy, identified roles and responsibilities, outline of initial and associated response actions, and the preparation of options for senior leader decisions. In addition, such planning can cut across agencies and promote integrated, consistent, and corresponding response actions that can be implemented, trained for, and exercised in a mutual direction. During a radiological theft or sabotage response, pre-planning will provide agencies the immediately benefit of understanding the following:

- Response objectives
- Interagency roles and responsibilities
- Interagency capabilities
- Initial and associated response actions (Office of Radiological Security, 2019)

2.2 TRAINING/ DRILLS AND EXERCISES

Conducting training exercises to ensure that the policies are sufficient is critical. Exercising our policies is important because the policy cannot be considered reliable until it is tested and has been proven to be practical, eliminating false assurances, which can compromise the integrity of a plan. Recommended best practices related to integrating and improving the coordination of law enforcement pre-event policy development, planning, training, and exercises include the following.

- Create opportunities for joint policy and planning sessions that focus on integrated policy discussions and joint planning among stakeholders, which will lead to joint policies and plans.

- Enhance training and exercises by creating tabletop and full-scale training/exercises focused on the response to an attack on a radiological shipment.

There are three primary methods that organizations can employ to exercise policies and procedures. The first is by using discussion-based exercises with all the involved parties. Discussion-based exercises are the most cost-efficient exercise to conduct and the easiest to prepare. They can be used at the policy formulation stage as a "talk-through" of how to finalize the plan. More often, they are based on a completed plan and are used to develop awareness about the plan through discussion. In this respect, they are often used for training purposes.

Secondly, the use of tabletop exercises is an effective method to evaluate policies. This type of exercise is particularly useful for validation purposes, particularly for exploring weaknesses in procedures. Tabletop exercises are relatively cost-effective to conduct. The Office of Radiological Security and the Federal Bureau of Investigation currently conducts tabletop exercises across the nation in an event called Isotope Crossroads. The purpose of the exercise is to focus on the security of radiological material during commercial transport. Each exercise is designed to promote information sharing, joint situational awareness, team building, and problem resolution in a crisis response situation.

Participants in these exercises include representatives from federal, state, and local law enforcement and emergency response agencies, public health organizations, transportation companies, and radiological material producing companies. Each scenario is customized to the specific location and challenges participants to work together in a scenario involving Category 1 and Category 2 radiological materials during commercial transit. Specific scenarios are exercised using actual transportation routes, transportation company response procedures, and various types and quantities of radiological materials transported through the local area of responsibility are explored (National Technology and Engineering Solutions of Sandia, LLC, 2018).

The last technique is to conduct a full-scale exercise. These events are a live trial of implementing a policy or procedure. Such exercises are particularly useful for testing logistics, communications, and physical capabilities. These exercises also serve as excellent training events in helping participants develop confidence in their skills and better understand what it would be like to use the plan's procedures in an actual event (Gov.UK, 2013).

3. CONCLUSIONS

Responding effectively and appropriately to a theft or sabotage event for radiological material is in the best interests of the public, industry, and law enforcement. By engaging both industry and law enforcement agencies early on, we can begin to build strategies that are effective at mitigating this threat.

This needed engagement will require some investments by industry in both physical security controls and administrative practices and for law enforcement in preplanning and training. However, by addressing these issues early on, these organizations and their leaders will have provided the tools to ensure that their organizations are best equipped to deal with this type of threat.

Law enforcement currently responds effectively to several different types of unacceptable events, but the response to radiological transportation threats is an area that needs further refinement. Now is the time to begin work, set goals, and go forward with the implementation of this strategy.

4. REFERENCES

Ananthanpillai, R. (2015, July 23). *Risk Mangement Monitor*. Retrieved from www.riskmanagementmonitor.com: http://www.riskmanagementmonitor.com/insider-threats-and-the-limitations-of-pre-hire-background-checks/

Concentric Security. (2009). *Recognizing Security Principles in the Access Control Point Design & Construction Process.* Retrieved from http://www.concentricsecurity.com/downloads/Recognizing_Security_Principles_ACP.pdf

Gitomer, S. J., O'Brien, H. A., Mason, C. F., Strub, T. L., & Van Tuyle, G. J. (2003). Reducing RDD Concerns Related to Large Radiological Source Applications. Los Alamos: Los Alamos National Laboratory.

Gov.UK. (2013, February 20). *Emergency planning and preparedness: exercises and training* . Retrieved from www.gov.uk: https://www.gov.uk/guidance/emergency-planning-and-preparedness-exercises-and-training.

National Sheriffs' Association. (2016, February 28). *EMBRACING TECHNOLOGY TO DECREASE LAW ENFORCEMENT RESPONSE TIME*. Retrieved from https://www.sheriffs.org/content/embracing-technology-decrease-law-enforcement-response-time

National Technology and Engineering Solutions of Sandia, LLC. (2018). *Isotope Crossroads*. Retrieved from https://isotopecrossroads.gov

Office of Radiological Security. (2019). *Radiological Theft Response Engagement Tabletop Exercise*. Retrieved from https://rsp.sandia.gov: https://rsp.sandia.gov/rtre-workshops/romania-rtre

Sandia National Laboratories. (2018). *Evaluation of Physical Protection Systems.* Retrieved from https://share-ng.sandia.gov: https://share-ng.sandia.gov/itc/assets/17-eval_pps_text.pdf.

US NRC. (2014). Physical Security Best Practices for the Protection of Risk-Significant Radioactive Material. Washington, D.C.