Proceedings of the 20th International Symposium on the Packaging and Transportation of Radioactive Materials

11-15 June 2023, Juan-les-Pins, France

EVALUATING AND COUNTERING THE INSIDER THREAT TO THE RADIOACTIVE SOURCE SUPPLY CHAIN

Dr. Justin Kinney
Oak Ridge National Laboratory

ABSTRACT

The modern supply chain is a global enterprise, and little drove this home more than the global COVID-19 pandemic, which sent economic shockwaves throughout the world. Many goods became scarce, as products were delayed, in limited supply, or simply not available. The suddenly diminished supply collided with still high demand and led to greatly increased costs. This was particularly true for the radioactive source supply chain. The pandemic introduced extensive delays for construction projects, slowed the transport of radiological materials to facilities, interrupted treatment deliveries, and impaired the mobility of contractors across the industry. All of these concerns not only adversely affected the economy but also impacted the safety and security of radiological material, potentially raising national security concerns. The vulnerability of the supply chain, a critical element in an increasingly interconnected world, was exposed. One example that challenged the adaptive capacity of the overall supply chain is the *Ever Given* container ship, which became stuck in the Suez Canal in 2021. This accident immediately shut down shipments that accounted for 12% of global trade, and long-term impacts are estimated to be much greater. Developing the ability to anticipate and react in real time to sudden changes has quickly become a necessity, particularly in industries that deal with the transport of hazardous material. The reaction to these dramatic incidents was to largely focus attention and resources on protecting the supply chain from external threats. However, the threat to the radioactive material supply chain from insiders intimately involved in the process may be even greater and remains a blind spot that requires increased attention. Recent events revealed the blueprint for targeting and disrupting that supply chain, so the potential for a malicious insider—or a manipulated, unwitting insider—to take advantage of this vulnerability is elevated, creating security concerns for radiological industries. This paper examines and analyzes the potential insider threat to the radioactive source supply chain and recommends steps to take to counter this possibility.

INTRODUCTION

Prior to the year 2020, the average person likely never put much thought toward the global supply chain. Unless one actively worked as a piece of that overall process, it simply wasn't something most people encountered in everyday life. Whenever one desired to purchase a specific product, they simply went to the store to find it on the shelf—or to a website online to place an order, rarely thinking beyond that shopping excursion to the process that produces and delivers a product to the store in the first place. The network that connects suppliers to factories to companies to stores, and

ultimately to the consumer, is overlooked. But that process, known as the supply chain, is as important as it is complex.

In the first days of the COVID-19 pandemic in early 2020, however, the concept of a supply chain became part of the daily lexicon for people around the world, as shelves once fully stocked routinely saw shortages of products, costs rose dramatically for many items, and delays became commonplace on everything from construction projects to delivery of goods. Even for those intimately aware of the supply chain process, its delicate nature and the ease/speed with which the system was compromised came as a surprise. Many had believed the globalized nature of the economy actually made for a more resilient system and argued that the more extensive and interconnected the web of trade, the less likely a break in one strand would impact the entire structure. And it's easy for some to dismiss the COVID-19 pandemic as a one-in-a-billion event; few incidents throughout history have so thoroughly enveloped the globe, invading every country, so surely you can't blame the supply chain for failing then, they might argue. Yet, the Suez Canal blockage shows this cannot be so easily cast aside. Instead of the complex web of trade holding the economy afloat, the interconnectivity may have inadvertently contributed to the disruption; by relying so heavily on international trade, a single vulnerable chokepoint like the Suez and Panama Canals or the Strait of Malacca in Asia—through which many transport vessels must pass—was enough to bring as much as 12% of the world's economy to a halt when faced with high winds. By creating interdependence between nations, the domestic capabilities needed to support the overall production of goods directly critical to a country has been eroded (Shih et al., 2021).

As with many materials and services reliant on the global supply chain, the radiological and nuclear industries are no different. Radiological materials are utilized in a variety of important products and supplies, including medical treatments, and are shipped around the world (Guarascio, 2021). Nuclear construction projects and parts shipments rely on a robust supply chain as well. An effective, efficient global supply chain is crucial for both new builds and operating/maintaining existing nuclear facilities (IAEA, 2021). Whether the world marketplace is affected by a pandemic, a transport ship runs aground, or another threat harms economic trade, the radiological and nuclear industries are likewise impacted. And while the world economy can certainly be stifled when such threats appear, the effect of delays, rising costs, or inability to procure materials also creates a potentially dangerous situation for both national and international security. These external threats are most visible and likely best understood, but the potential risk from an insider threat is just as concerning. Yet, sometimes this risk can unfortunately go overlooked due to the relative level of trust placed on insiders. This blind spot toward the insider danger is an area that requires examination.

SUPPLY CHAIN GLOBALIZATION

Decades to centuries ago, the world's economy was localized and not well connected. Usable goods were limited to products that could be locally grown and/or produced. What trade did exist was primarily between immediately neighboring countries. There was, of course, minimal exchange between nations on that larger scale (e.g., spices or silk from Asia reaching Europe), but this was the exception for the large majority of goods and materials. It simply was not feasible to extend a country's trading empire that far due to the extensive time constraints it demanded, travel and shipping difficulties, and technological deficiencies. But as the world's population grew and innovation began to prosper and thrived, the trading market expanded along with it.

Today, the world's economy is more interconnected than it has ever been. Goods and materials are shipped around the world as even a single finalized product can be sourced, in part, from several different countries, assembled in another, and then sold and distributed worldwide. The ease with which people and materials are able to move around the globe has dramatically increased as new innovations and technologies brought far-flung corners of the world together.

This amplified globalization has had a variety of impacts, such as driving prices down because of the ability to more cheaply source items from new regions, but it also created an increased dependency between nations. This dependency is not necessarily bad and may have national security implications, as some theorists posit the worldwide decrease in major power wars over the last several decades is, at least in part, due to nations needing one another for trade purposes. But the loss of independence does create new problems as the reliance on foreign regions for goods also makes a nation susceptible to problems that arise in those foreign countries. For example, closing a single pipeline—in combination with a few other events—can create deeper dependence on receiving oil and gasoline from abroad. When supply chain and other issues arose in those regions, gas prices began to dramatically rise.

This wave of globalization is unlikely to ever disappear. The world is connected now and, barring some catastrophic event, a reversal of those interwoven relationships is unlikely and perhaps impossible. It is true that fluctuations in certain industries may occur as new administrations enter and leave office, supply and demand evolves over time, or political trends and ideologies morph throughout the public consciousness, but connective technologies and products have linked the world in permanent ways, for better or for worse. The supply chain will consistently require attention when it comes to finding means of protection, from both external and internal threats.

EXTERNAL THREATS

When people think of threats to the supply chain, the typical visual is from the outside. Derailed trains, ships run aground, or even—most recently—a worldwide pandemic shutting down factories and more, are common considerations. And it is true that such events can have clear and significant impacts to the efficiency and connectivity of the supply chain. We have seen this at work on many occasions.

Although the COVID-19 pandemic and its well-documented impact on the global marketplace is probably the most notable, the *Ever Given* transport ship getting stuck in the Suez Canal is probably an even better example of the delicate nature of the supply chain and the global damage even a relatively small, localized event can cause when things go wrong.

The *Ever Given* is one of the largest container ships in the world, with a length of nearly 400 meters. In March 2021, the *Ever Given* was traveling from Malaysia to the Netherlands, which required passage through the Suez Canal, a 193-kilometer artificial waterway in Egypt connecting the Mediterranean and Red Seas. The Suez Canal is one of the world's most important trade routes, as approximately fifty ships per day travel through it, accounting for roughly 12% of the total globe trade at the time of this incident (Harper, 2021). However, despite its importance and traffic, much of the canal is a single lane roughly 220 meters wide, meaning it cannot handle two ships passing in opposite directions at the same time. On this particular day, high winds (>45 mph) caught the *Ever Given*'s crew by surprise and nudged it off course while inside this narrow waterway. The crew lost

ability to steer the ship; it quickly ran aground and was turned sideways, blocking the canal entirely. At that size and weight, gusts of wind caused the containers to act as a sort of sail and any momentum can be difficult to counteract. It took six days before the vessel was cleared and the canal reopened for passage.

This relatively quick and simple event—a ship getting caught in the wind and blowing off course—was devastating to the global trade market. *Lloyd's List* estimated that the value of the goods delayed each hour was $400 million and that every day to clear the obstruction would disrupt an addition $9 billion worth of goods (Harper, 2021). This obstruction affected global prices—particularly oil—and resulted in delays in the delivery of goods (e.g., semiconductors) as ships were either forced to wait or find alternate routes, and this event raised concerns about piracy and other security concerns with the unusually high concentration of valuable goods in a small area.

With regards to the *Ever Given* incident, most of the public impact was experienced in delays and higher prices for material goods and oil. Two military ships were caught in the blockage chaos as well, but otherwise, most of the maritime vessels impacted at the Suez Canal were either oil tankers or container ships carrying various commercial products. However, this view of the supply chain is limited and incomplete. It is more than store-bought goods that consumers purchase; as harmful as that disruption can be, commercial items might not be the only targets of a threat. The radiological and nuclear industries also undergo supply chain processes for delivery of various medical treatments, reactor materials, contractor mobility, construction, and more (World Nuclear News, 2021).

These external threats exposed the vulnerabilities of the global supply chain matrix. Its complexities and interconnected nature can be susceptible to shocks to the system, large and small. Both the pandemic and the *Ever Given* situation were unintentional attacks; neither was planned or premeditated. Neither specifically sought to target the delicate balance of moving goods from suppliers to consumers. Yet, external threats can also be malicious, attacks from individuals or groups seeking to cause harm. Surely, many who harbor extremist beliefs were paying attention; they witnessed how easily the global supply chain can be crippled and the economic damage it can do in only a few short days, much less months or years. They will be watching closely to analyze the nuances of those events. It is not farfetched to presume they might one day seek to duplicate those negative effects as a way to seed chaos and destruction.

There are a couple primary ways a group of extremists could approach this. First is what most think of when discussing extremist or terrorist groups, the physical attack—a bombing of a ship, a missile strike on a trade-heavy waterway or chokepoint, an assault on a product factory. Historically, terrorist organizations seek out populated areas or symbolic structures (e.g., a church or government building) to cause immediate, newsworthy destruction and human casualties. But organizations evolve and after witnessing the long-lasting and widespread chaos a supply chain disruption can create, it is reasonable to assume that tactical targets might also shift. However, the security processes for protecting the supply chain are largely the same for protecting anything else. Transport security is more spread out, more mobile, and more exposed, but physical security measures have a long history of research and implementation.

The second, and more insidious, way an extremist might seek to disrupt the supply chain is significantly more overlooked but has potentially a larger impact: the insider threat. An insider

introduces the potential for groups to either manipulate unwitting employees or to recruit malicious ones—using their strategic access, authority, or knowledge—to engage in sabotage, theft, or other disturbance of some key supply chain step.

INSIDER THREAT ANALYSIS

External threats are usually observable, easily understood, and typically accounted for in protective measures and common security best practices. Even when an unanticipated external threat arises like the COVID-19 pandemic, any lessons learned typically focus on how to prevent the next external threat. Yet, there is reason to believe the vulnerabilities exposed by external threats may face a different—and potentially more devastating—kind of danger from those seeking to exploit the holes poked in the perceived resilience of the supply chain system. Especially when dealing with the movement of radiological or nuclear material and equipment, those vulnerabilities carry a unique and critical risk.

Most experts assumed the interwoven nature of the global marketplace would prove resilient and mitigate dangers from a threat, so there was little reason to consider the risks an insider might pose. But the last two years revealed that was not the case. The entire perspective must be reevaluated because those in security surely were not the only ones to notice how fragile the system truly is. Plenty of others, from terrorist organization to disgruntled employees had to recognize that it did not take much—a single stuck boat, for instance—to bring the trading economy of countless nations to a screeching halt. Even at a simplistic level, it would not be difficult for a trusted insider on a transport ship carrying radiological material to believably feign losing control of the vessel in high winds, creating a similar scenario to the *Ever Given* in one of several different chokepoints. And there are a myriad of other ways an insider could act as well.

Insiders are particularly hazardous to an organization or a process because their status gives them access, knowledge, or authority to create disruption that someone from outside cannot obtain on their own. They can act in ways that may seem normal or permitted because of their role in the process, but will lead to deleterious, costly, or even dangerous outcomes. In an industry with inherent risks like the radiological or nuclear spheres, these insiders in trusted positions have undergone background checks or clearance investigations and are responsible for handling, processing, or controlling important steps.

An important thing to remember is that insiders are not necessarily direct employees (or former employees). Within the radiological supply chain, especially, there are many moving parts including different companies, suppliers, and other third-party entities. Not all organizational links in the supply chain will have required the same level of background checks and security procedures on their employees; perhaps one foreign vendor doesn't have access to a reliable, national database to investigate a potential employee's criminal history, for example. It is extremely difficult to maintain security, accountability, and transparency in the global supply chain when outside suppliers—especially when finding and purchasing spare parts—may not have seen the same scrutiny processes prior to hiring or during transport procedures.

Sometimes insiders play an unwitting role; whether due to negligence, lack of attention to detail, fatigue or illness, or poor training, these people act in unintentional, but still harmful manners, such as failing to check an alert because they have experienced many false alarms in the past. Sometimes other insiders act maliciously but alone, such as disgruntled employees seeking to enact

revenge on the organization, achieve personal satisfaction, or build their own egos. Other times, they volunteer or are recruited to act on behalf of outsiders who do not have the same access, knowledge, or authority. In these situations, it can also take a myriad of motivations, from ideological agreement to financial hardship and stress to seeking meaningful purpose. And situations with economic and social pressures—as we have seen with the recent COVID-19 pandemic—can exacerbate psychological stressors. But in every case, that insider exploits the trust and responsibility the organization places on them and acts to either steal information or sabotage materials/processes. Yet this is frequently a gap in security training or awareness—perhaps due to the lack of understanding of behavioral studies in more physical science fields—and that oversight needlessly creates a heightened level of risk, both to the economy but also to national/global security. Steps need to be taken to deter, mitigate, or better respond to the radiological supply chain insider threat potential through better training, behavioral study of past insiders, and technological fail-safes.

RECOMMENDED ACTIONS

There are common best practices to protect the international radioactive source supply chain, but there are a few additional recommendations to further target this issue and address the vulnerabilities an insider could exploit.

Recommendation 1: Invest in employee training on insider threat awareness

One of the best weapons against insider threats is simple awareness. From the work environment to your fellow coworkers, it is vital to remain alert and to know what indicators of a threat look like. These indicators might be something obvious, picked up in a standard background check, but it is not always so clear. It can be particularly difficult for someone in an executive position or in human resources to recognize signs when they are not engaged with individual employees on a daily basis. However, no one is in a better position to recognize and identify signs of aberrant behavior or early warning indicators than one's peers.

Employees are always trained for their specific job, but one area that is often overlooked in building a positive working environment is to foster better employee relations with one another (Fatima et al., 2013). When employees get to know one another well, they are quick to recognize when something seems aberrant, or out of the norm. When employees are trained in specific insider threat indicators, they are equipped and empowered to view aberrant behaviors as potential concerns. This is not to suggest a company should weaponize employee friendships or turn the office into a police state. That approach would surely backfire because it would disincentivize the very thing needed: people building relationships. But sometimes, all that is needed to prevent an insider threat from manifesting is to have someone notice when an employee is struggling personally (e.g., financial distress, family trouble, workplace complaints) and reach out a helping hand. And when employees feel they are being supported, helped, and recognized, this increases commitment and loyalty to the organization (Ministero, 2021). While this may not eliminate all threats—some individual ideological causes can outweigh the benefits of a positive organizational environment—it does help lessen the risk of employees turning on their employer. When needs are fulfilled, employee relations are high, and individuals feel appreciated, the insider threat risk is reduced as well (Shoss et al., 2013; Sulea et al., 2012)

Further, in the event that an insider threat does begin to proceed, empowering employees with the knowledge and authority to speak up anonymously would provide another barrier and disrupt plans.

While this could lead to false alarms from employees who mean well, yet inaccurately assess the situation, it still acts as a valuable initial warning system for potential threats; these reports would need to be investigated to assess validity. However, this pathway to report must not be viewed as a punitive means to go after employees; at this stage, it must be used as a way to help those who are struggling and improve the lives of those in the workforce.

In a supply chain that is increasingly global and interconnected, employee connections are becoming more vital to understand and cultivate. Because it is not just the employees within a single company who must be secure, but in every link in the chain, many employees who have not been vetted through typical security measures or who never directly interact with security or management. This is important to mobilize that workforce engaging at interactive levels and empower employees to act and react to changes, shifts in behavior, or anything else that stands out.

Thus for any industry looking to mitigate and deter potential insider threats, providing employees with two things are a must:

1. Knowledge and awareness to recognize signs via training procedures
2. Authority and a pathway to react to those signs appropriately and with care

Recommendation 2: Initiate behavioral science programs to examine past insider threats and learn from their actions. Create a framework to study insider attacks to the radioactive source supply chain

Behavioral science is a branch of study that is often ignored in favor of physical security. But the insider threat is a unique challenge because by definition, insiders are often able to bypass physical security using the nature of their access, authority, or knowledge their role within the organization allows.

The psychology that drives insider threats is overlooked. Yet a better understanding of their motivations, and developing methods to address and mitigate them, would be excellent security measures. Good behavioral science or observational programs will learn and adapt from past incidents, using known cases to inform future ones. By looking back to identify indicators in hindsight, organizations can use those and recognize their emergence as future predictors. There are certainly broader studies that have done this, but each facility, each transport vessel, and each supply chain process is distinct and presents its own challenges, vulnerabilities, and opportunities. This is why lessons learned from varying industries cannot be used interchangeably without taking the time to individualize it. There are important values and principles that can be drawn from other industries, but it is vital to incorporate them only in context and in concert with the unique elements of a radioactive source supply chain network.

The value of building an insider threat framework specific to this supply chain will help clearly define a variety of variables. Frameworks may include technical and behavioral elements, tangible attack types, and personal motivations, as well as human factors that lead to unwitting insider threats, so a well-designed framework can act as a model for understanding the threat and discovering patterns, as well as for predicting future ones.

Recommendation 3: Install both technological and administrative fail-safes

The supply chain is a complex web of different people, organizations, shippers, security measures, and products. It is perhaps understandable how an unwitting insider might slip up when attempting to keep track of it all, leaving themselves or the organization vulnerable to exploitation. Fatigue,

illness, inadequate training, distraction, or any other means could all lead to a simple, yet damaging, mistake. One way to strengthen security, mitigating the risk of such mistakes, is for an organization or process to install fail-safe measures.

There are two primary types of fail-safes in these cases: administrative and technological. Examples of technological measures include utilizing ID cards and password checkpoints. Each lock or barrier that must be consciously bypassed—even small ones like scanning a badge—requires an individual to physically and mentally pause and consider their actions. Turning these procedural steps into conscious decisions and actions minimizes the risk of unwitting insiders. Further, when these actions are tracked, monitored, or logged into a computer system, it deters malicious insiders as well and provides oversight for the various steps and strengthens access control. This should particularly be involved in any situation when material is being moved or changing hands. The radioactive source supply chain notably includes many people as material is moved around the world; each transfer is a link in a chain that can feasibly be broken and requires security. For materials that necessitate a security clearance or other background investigation, such as access to nuclear or radiological material, these fail-safes become even more important to guarantee that everyone in the chain of custody is vetted and barriers remain safeguards.

On the other hand, administrative defenses are more personal and utilize the principles of psychology and understanding people. Empowering employees to be aware of their surroundings through additional insider threat training is a strong place to start, but administrative safeguards involve more than training. Compartmentalization of information, authority, and physical areas keep any single individual from knowing too much or having too much access. This strategy helps limit the damage one insider could inflict on their own. Implementing a two-person rule avoids the problem of employees accessing secure areas alone or unsupervised. Having an escort present is particularly important in a complicated supply chain system because it guarantees there is always at least one person present who has undergone security and background checks that can be verified and trusted. Ongoing, periodic trustworthy checks monitor motivational factors like financial troubles, rising psychological issues, dependency or addiction problems, or anything that might give an external adversary leverage over the employee.

For those involved in the radioactive source supply chain, implementing both administrative and technological measures as fail-safe procedures will ensure a safer, more secure process. The combination addresses physical security and creates behavioral deterrences against insider threats. For materials that require utmost care due to their sensitive nature, like in radiological or nuclear industries, these safeguards protect more than just economic or market interests, but also act in service of national or global security.

CONCLUSIONS

The global supply chain, once thought to be strong and resilient, has suffered multiple major setbacks in the last two years. The *Ever Given* transport ship getting stuck due to high winds shut down nearly 12% of worldwide trade, and the lingering COVID-19 pandemic has resulted in delays, empty shelves, and an inability to procure products. All told, these problems have cost billions of dollars in lost revenue and repairs. While no one thought the supply chain was impervious, its interconnected nature was thought to protect against shocks to the system. Yet these shocks sent rippling waves that reverberated throughout the world, affected every country, and everyone noticed, even those lucky few who may not have been directly hurt.

Further, it is naïve to think that only those with honorable intentions who wish to strengthen and secure the supply chain noticed. Many who seek to cause harm also surely recognized what had happened. And although the response to past—and ongoing—threats has focused much attention on beefing up physical security to protect from future external threats, the risk of an insider threat is also at an all-time high and potentially brings even more damaging consequences. Whether an external adversary hopes to recruit and exploit an insider's knowledge, access, or authority, or an employee already on the inside chooses to act alone as a means of revenge, it is vital to take steps to deter, counter, and otherwise secure the radioactive source supply chain from these dangers.

These steps could involve dedicated investments in training employees to recognize early insider threat indicators, the implementation of behavioral science programs to create insider profiles and learn from past threats, or installation of joint technological and administrative fail-safes to bolster physical security against vulnerable gaps and deter individual acts. The insider threat to the radioactive source supply chain is elevated now more than ever, as the last two years have reinforced just how important it is to the world economy and daily life, but also its susceptibility to attack.

REFERENCES

Fatima A., Iqbal M. Z., & Imran R. (2013) Organizational commitment and counterproductive work behavior: role of employee empowerment. In: Xu J., Yasinzai M., Lev B. (Eds.) *Proceedings of the Sixth International Conference on Management Science and Engineering Management*. Lecture Notes in Electrical Engineering, vol 185. Springer, London. https://doi.org/10.1007/978-1-4471-4600-1_57.

Guarascio, F. (2021). EU may face shortage of key materials for diagnostics, cancer treatments. *Reuters*. Published December 7, 2021. https://www.reuters.com/world/europe/eu-may-face-shortage-key-materials-diagnostics-cancer-treatments-2021-12-07/

Harper, J. (2021). Suez blockage is holding up $9.6bn of goods a day. *BBC News.* Published March 26, 2021. https://www.bbc.com/news/business-56533250

International Atomic Energy Agency (IAEA). Management of the nuclear supply chain. Accessed December 10, 2021. https://www.iaea.org/topics/management-systems/management-of-the-nuclear-supply-chain

Ministero, L. (2021, September). Developing an organizational commitment measure for insider risk [Online webinar]. The Counter-Insider Threat (C-InT) Social & Behavioral Science (SBS) Summit 2021, Virtual Engagement. https://sbssummit.com/videos/developing-an-organizational-commitment-measure-for-insider-risk/.

Shih, W.C., Huckman, R.S., & Wyner, J. (2021). The challenge of rebuilding U.S. domestic supply chains. *Harvard Business Review.* Published May 26, 2021.

Shoss, M. K., Eisenberger, R., Restubog, S. L. D., & Zagenczyk, T. J. (2013). Blaming the organization for abusive supervision: The roles of perceived organizational support and supervisor's organizational embodiment. *Journal of Applied Psychology*, *98*(1), 158–168. https://doi.org/10.1037/a0030687.

Sulea, C., Virga, D., Maricutoiu, L. P., Schaufeli, W., Zaborila Dumitru, C., & Sava, F. A. (2012). Work engagement as mediator between job characteristics and positive and negative extra-role behaviors. *Career Development International*, *17*(3), 188–207. https://doi.org/10.1108/13620431211241054.

World Nuclear News (2021). International event focuses on nuclear supply chain. Published September 21, 2021. https://www.world-nuclear-news.org/Articles/International-event-focuses-on-nuclear-supply-chai