Proceedings of the 19th International Symposium on the Packaging and Transportation of Radioactive Materials
PATRAM 2019
August 4-9, 2019, New Orleans, LA, USA

THE USE OF EMERGENCY EXERCISES TO PROMOTE A CULTURE OF SECURITY AND RESILIENCE

Philip Murphy
Direct Rail Services

ABSTRACT

The mission of the Nuclear Decommissioning Authority (NDA) is to decommission and clean up the legacy of the UKs Civil Nuclear sites. As a subsidiary of the NDA, Direct Rail Services' (DRS) strategy is to provide a long-term capability to meet the lifetime requirements of their 120-year nuclear mission.

DRS, as a provider of nuclear transport services, must demonstrate and encourage the highest standards of security, conforming to the requirements of statutory regulatory bodies such as Office of Nuclear Regulation – Civil Nuclear Security (ONR-CNS), Department for Transport (DfT), Ministry of Defence (MOD) and Office of Rail and Road (ORR), and the NDA.

As nuclear material leaves a highly secure nuclear licensed site this inevitably brings an increase to the risk of a security event occurring. Whilst security focus is integral to all activities in the nuclear industry, transportation of radioactive materials outside of licensed site boundaries onto public infrastructure brings with it different challenges.

In the twenty-first century, security is one of the most tested industries due to the threat from international terrorism. Whilst intelligence suggests that, an attack against the civil nuclear industry is low; a physical or cyber-attack against the transport industry remains a significant risk. DRS lead or participate in a number of emergency exercises providing our trained commanders and 24/7 control room personnel with an opportunity to practice using our emergency/incident response plans. Emergency exercises are scenario based around a plausible incident, these have included:

- Major fuel spillage
- Protestor activity
- Major incidents on CAT III nuclear services.

DRS have well-rehearsed and exercised procedures when dealing with incidents on any of its train services, locations or facilities around the country, with emphasis on the movement of nuclear material by rail. The procedures incorporate lessons learnt from previous exercises, incidents and any changes in regulation or legislation.

The aim of this paper is to demonstrate how the implementation and practice of security and resilience exercises mitigate risk, improve decision-making and enhance operational reliability to satisfy regulatory requirements, whilst promulgating and promoting a positive security and resilience culture to provide an effective and robust response to any emergency scenario.

INTRODUCTION

Security in the twenty first century is an ever-changing dynamic. The threat from terrorist activity is real, and an incident could happen to anyone, anytime, anywhere. As a transport provider, operating in two of the most heavily regulated industries in the UK, rail and nuclear, DRS continuously improve upon its security arrangements, from a physical, personnel and information perspective. Resilience and business continuity are just as important and testing and exercising processes is a vital commodity of promulgating a positive security and resilience culture. Security in the nuclear industry is of vital importance, and whilst intelligence suggests that an attack against the industry is unlikely, there is a risk that nuclear material could be used in criminal or intentional unauthorised acts, creating a threat to security [1].

Traditionally, organisational security has often focused on a security policy rather than focusing on the development of a security culture [2]. DRS' aspiration is that our business operations will cause no harm to any person either directly or indirectly. In order to achieve this, DRS have implemented, and reviews annually, a series of emergency/incident response plans. With any emergency, the human factor sometimes cannot be judged. Nobody knows how he or she will react in a situation until it happens to him or her. By delivering emergency exercises that both tests procedures and personnel, DRS encourages and has embedded an organisational culture that recognises and promotes the importance of security.

Regulatory compliance with the necessary security arrangements is a key requirement for DRS in maintaining its Class A carrier license allowing us to continue delivering the NDA mission [3]. DRS emergency/incident response plans apply to all personnel who have a responsibility to respond to an emergency/incident, by providing a formulated and structured response to ensure people are safe; assets, including the nuclear material, are secure, minimise impact on the business and aid a speedy recover to 'business as normal'. DRS play an active part in either leading or participating in emergency exercises, which are based around security or non-security based plausible situations that could realistically happen. Key working relationships with British Transport Police (BTP), Network Rail, Civil Nuclear Constabulary (CNC), Electricite de France (EdF), Magnox, RADSAFE and other stakeholders have been formed, which are crucial in the unlikely event of an incident occurring.

DRS is the only operator in the United Kingdom approved to undertake movement of nuclear material by rail and have completed more than five million miles of successful transport without any incidents involving the release of nuclear material and as a result, DRS' knowledge and experience of transport in the nuclear industry is world leading. Typically, safety and security have been treated as separate disciplines, but researchers are beginning to argue that if "it's not secure, it's not safe" [4]. DRS' company strapline of 'safe, secure, reliable' provides strategic alignment to providing a long-term capability to meet the lifetime requirements of the NDA 120-year nuclear mission [3].

THE CHALLENGES

Security incidents within the nuclear industry are thankfully rare. High-profile terrorist attacks on passenger rail services in Madrid, London and Mumbai provide troubling illustrations that public transportation systems are a vulnerable target for terrorists. Rail freight conveying toxic chemicals and nuclear material often has minimal security as it passes through heavily populated areas therefore increasing the potential risk of a security incident occurring [5]. Within the UK, the horrific attacks

on London and Manchester in 2017 served as a reminder of the continued threat that terrorism poses. The threat is real and, as with safety, security is everyone's responsibility.

In the absence of real-life security incidents against the nuclear industry, systems and processes put in place have a greater potential to remain untested for a significant time. With this in mind, ensuring that an organisation can respond effectively to an incident is critical, and DRS have implemented effective security emergency preparedness and response arrangements, which are integrated with the wider health, safety, environmental, and quality arrangements.

One of the biggest threats to security is that related to a cyber-attack. This threat is constantly evolving, and research suggests that cyber systems are likely to contain vulnerabilities through insufficient protection. Information technology has become an integral part of modern life [6]. The regulatory, reputational and financial implications of a successful cyber-attack could be crippling. Mitigating this risk is not easy, but understanding the risk and the establishment of an information security culture is necessary for effective information security [7]. From a business perspective, DRS challenge the cyber threat through internal cyber security awareness campaigns including measurement of click rate against spam emails and improvements upon detection capability. Both challenges are aimed at mitigating the board level risk of a cyber-attack, and are dealt with by our in-house IT and Information Security capabilities.

Security exercises enable DRS to validate training and practice procedures, decision-making, command, control, tactics, and response arrangements in a challenging but safe way. The challenging approach makes those involved in an exercise "think on their feet" whilst always testing procedural control to remove the human element being the greatest risk to security.

In order to mitigate the risk and threats faced, DRS has effective guarding and policing arrangements, which integrates the operations of relevant police forces – Civil Nuclear Constabulary (CNC), Local Police forces, Police Scotland and British Transport Police (BTP) – and security guard services. All exercises provide excellent learning and potential changes to procedures. A key learning point from one multi-agency exercise, which DRS led, was a change to Police processes to allow railway personnel into a cordon to make-safe the operational railway. Without this exercise, this key learning point may not have been shared, increasing the likelihood of a problem occurring in a real-life situation and delaying a response.

Whilst all exercises are effective in reducing the risk against terrorist attacks, there are other threats that DRS must be aware of and prepare for. The most realistic threat facing the movement of nuclear material is anti-nuclear demonstrators who peacefully protest against the nuclear industry. Again, the close working relationships with policing agencies provide a sharing platform for intelligence and a collaborative working practice against the threat.

As described above, the threat is both operational and non-operational for railway movements. Being able to test and exercise plausible scenarios ensures that emergency/incident plans are robust enough to give organisations the opportunity to undertake objective assessments of their capabilities and performance, as well as identify areas for improvement [8].

Whilst security exercises are generally based around a threat relating to some form of attack, DRS' emergency/incident plans must be able to stand up to natural disasters, such as flooding, heavy snow and high winds. Recently, domestic political issues have raised a cause for concern, with threats posed directly against the railway. All of our plans must be able to be reactive to different situations and exercising the plans regularly allows the processes to be fit for purpose.

As a business, DRS have an identified risk of a "major safety or security incident". Taking into consideration that all of DRS' nuclear material transportation is conveyed on UK mainline rail infrastructure and through heavily populated areas, the toleration of this risk is fair and minimal. The railway is part of the UK's critical national infrastructure (CNI) which the UK government define as "those critical elements of infrastructure of which the loss or compromise of could result in a major detrimental impact of essential services or a significant impact on national security" [9]. Being defined as CNI provides peace of mind to members of the public that transportation of hazardous goods be protected by the UK government, ensuring that protective security is in place for critical assets.

THE HUMAN ELEMENT

Before sailing the Titanic, Captain E J Smith famously said, "It will never happen to me". With this in mind, take into consideration that on a given day in New York City, more people pass through Penn Station than all three major airports servicing the region combined. This number of people, combined with the required need for easy access, makes securing passenger railways a daunting task. If you add the transportation of nuclear material through a major railway station whilst there are thousands of people in the vicinity, the vulnerability provides terrorist organisations with an opportunity to cause mass chaos, with very little planning and preparation. The thought process of Captain Smith comes into play here as the vast majority of people will adopt similar thought processes and believe that they will go through their lives without experiencing an incident such as the Manchester Arena attack. It must be argued, however, that this thought process is not prevalent within the nuclear industry, and the IAEA recognises that human resources development is the "cornerstone of capacity building and nuclear security skills" [10]. Within the rail industry emergency exercises are also used as a way of demonstrating readiness to deal with major incidents. In many multi-agency exercises that are carried out each year the aim of the organisations taking part "is to provide an integrated approach to incident management, response and investigation, piecing together each individual organisations emergency plans" [11].

Resilience professionals provide 'what if' scenarios enabling organisations to practice their response arrangements, learn from exercising and improve processes accordingly. This valuable experience provides a low-risk environment to test and familiarise personnel with roles and responsibilities and foster meaningful interaction and communication across organisations.

Another factor to consider is the threat from inside an organisation. The insider threat is always present and in many ways, provides the greatest threat to any organisation as the human factor sometimes cannot be predicted. This threat is real and is here to stay. In the USA, the National Infrastructure Advisory Council [12] highlights that awareness and mitigation of insider threats varies greatly among companies and sectors and is often dealt with poorly [13]. In order to protect against this threat and as a licensed duty holder, all personnel at DRS are vetted prior to joining the organisation and are security cleared to a level, which is appropriate to their role. Security aftercare is also a vital part of ongoing personnel security providing information to highlight potential insider activity. Recently, senior leaders at DRS attended a training course ran by the British Transport Police (BTP) on the insider threat; this provided a great opportunity to share knowledge, understand the threat and review processes. There are many international case studies of an insider threat and, whilst DRS have never focussed an exercise on this topic, close working relationships with industry partners maintains the realism of this threat and strengthens the internal measures in place to reduce it.

LEARNING FROM EXPERIENCE

A disaster, natural or deliberate, or an accident? How do we acknowledge which it is? What emergency/incident plans do we have? Or do we treat any incident, irrelevant of its cause, the same way? As intelligence suggests that an attack against a nuclear rail movement is low, all incidents that DRS are involved with need to be treated the same, with security of nuclear material of paramount importance.

Unfortunately, processes can be reviewed following an incident, which has caused a loss of life. United Nations Maritime Agency re-examined international safety regulations for large passenger ships in the wake of the Italian cruise liner disaster in 2012. DRS prides itself on high levels of performance and quality [14]. Statistics of the Rail Safety and Standards Board (RSSB) [15] show that the UK rail industry's safety performance has steadily improved over time due to learning from near misses and incidents, in a process known as learning from operational experience. The opportunity to learn and the willingness to reflect from the RSSB resulted in lives being saved in the last fatal passenger train accident at Grayrigg in 2007; the crashworthiness of the train involved and the laminated glass used in its windows was the culmination of in-depth research and learning from previous rail accidents [16]. The learning from operational experience concept can allow rail operators, such as DRS to "do it right the first time" [17].

How can learning from experience improve a security culture? The American entrepreneur, Tim Ferriss, defines culture as:

"What happens when people are left to their own devices"

The CEO of Security Journey, Chris Romeo [18], argues that this can also apply to security culture by injecting the word 'security' in to the definition:

"Security culture is what happens with security when people are left to their own devices"

Emergency exercises provide a safe learning environment for all of those involved. Each exercise that DRS have taken part in has provided some learning; the key is to ensure that the same learning point does not keep repeating itself. Without the opportunity to exercise emergency/incident plans with other stakeholders, would not allow DRS to embed the importance of nuclear material involved in an incident. Romeo's [18] definition would provide great description of the event if the plans had not been rehearsed; each stakeholder would be left to their own devices and there would not be any structure to the emergency response.

Exercising is only one way of enhancing a security and resilience culture. DRS' long term corporate strategy is to take holistic approach to ensure effective coverage of the main pillars of total security. Security is everyone's responsibility and DRS continue to ensure that all members of personnel are trained, briefed and exercised when and where a requirement is identified.

EMERGENCY EXERCISES AND BUSINESS CONTINUITY

The final Communique of the 2016 Nuclear Security Summit stated that the threat posed by nuclear and radiological terrorism "remains one of the greatest challenges to international security, and the threat is constantly evolving" [19]. This statement, along with the unfortunate incidents as described earlier, highlights further the importance of putting in place measures to prevent, detect and respond

to an act of terrorism and, consequently, to ensure that adequate resources are assigned to establish and maintain robust nuclear security measures worldwide [20].

As DRS work in heavily regulated industries, a number of regulations state that coordinated measures and response management are required in order to manage a business response to any type of incident effectively through its emergency, incident, contingency and business continuity plans. Planning for responding to incident situations ensures that all organisations involved in the response can communicate and coordinate their efforts, improving not only the management of the scene but the incident recovery process.

DRS use a three-year rolling exercise plan to ensure that the ever-changing security threat in the twenty-first century is tested regularly. However, testing procedures and emergency/incident plans are not always focussed around security as health, safety and environmental scenarios are also exercised.

A gold-silver-bronze (Figure 1) command structure is a hierarchy used for major operations by the emergency services of the UK.

Figure 1 - DRS Command Structure

DRS use this recognised command structure in managing emergency/incidents internally, with gold command undertaking strategic command, silver being tactical command and bronze being operational command. All relevant commanders will communicate and coordinate with their counterparts at other organisations.

Within a short period, emergency exercises at DRS have come a long way; from a simple discussion based exercise to a more challenging live exercise, involving an evacuation of a passenger train. The more varied and challenging scenarios keep operational, tactical and strategic commanders in a heightened state of readiness, making the exercise much more realistic and plausible.

An emergency/incident can happen on the operational railway at any time. With this in mind, having competent people within an organisation who can undertake roles to respond is crucial. Over the last 12 months, DRS have increased the numbers of people who receive training across the UK in line with business requirements. Increasing the amount of people that can undertake such roles is critical in ensuring that an organisation remains resilient to such an incident. This involves new people to the organisation, those that have been promoted, and those, more importantly, who have been in position for a long period. This competency-based activity requires a positive security and resilience culture, which mitigates risk, improves decision-making and enhances operational reliability to satisfy regulatory requirements. This activity also lends itself to increasing the quality and frequency of training and exercising, which relates to it being a measurable target.

Emergency exercises are a key business target for DRS and, as such, progress is reportable to both the Board and the parent company. DRS' independent Security and Resilience department endeavour to use the exercises as a way of embedding a positive security and resilience culture, addressing and mitigating risks by working closely with all other internal departments, stakeholders, supply chain and wider industry partners to implement regulatory and technical security and resilience. Any learning from an exercise is captured and shared appropriately and an independent regulator assesses at least one emergency exercise per annum. Indeed independent regulators have been invited to attend emergency exercises in order to obtain in-depth feedback and share our work with other organisations.

Any organisation in any part of the world is susceptible to a natural disaster. The Federal Emergency Management Agency (FEMA) states that between 1976 and 2001, 906 major disasters were declared in the United States. Without preparation and in essence a 'Plan B', disasters can close a business down and studies show that 43% of companies hit by severe crises never reopen [21]. Causes of business interruption are not only from natural disasters, but could be because of human error or malicious threats from outsiders. The threat of cyber-terrorism can be as destructive as physical acts of terrorism [22]. Whilst emergency/incident plans are crucial in the response phase, business continuity plans are just as important in seeking to eliminate or reduce the impact of a disaster / disruptive incident before it occurs.

There is no single recommended plan for business continuity; instead, every organisation needs to develop comprehensive business continuity plans based on its unique situation. Over the next 12 months, DRS will implement and thereafter maintain a robust Business Continuity Management (BCM) system that will enable prioritised activities to continue to deliver key services in the event of a disruptive or crisis situation.

The system will include Directorate / Department BCM teams, Business Continuity Plans (BCP) and other associated documents, BCM Activation, Escalation and Stand Down procedures that align with the DRS Emergency Plans, an internal DRS BCM Training Course and DRS Awareness Programme for all employees.

The internal DRS BCM course will provide attendees with the required training, advice and guidance to analyse their Directorate / Department and create appropriate business continuity arrangements that will be regularly reviewed. Planning assumptions will be that it is not about the cause of the disruption but the effect it will have on DRS prioritised activities, with the emphasis being on determining appropriate resumption strategies that can mitigate a wide variety of disruptive incidents.

The internal DRS BCM Awareness programme will be attended by identified personnel who will gain a clear understanding of what BCM is, why it is a requirement for DRS, what arrangements are

in place and what they need to be aware of in relation to their Directorate / Departments BCM arrangements and how to react to a disruption.

Through use of the internal DRS BCM course, Awareness programme and exercising of the BCM system, over time this will build, promote and embed an ongoing positive BCM culture within DRS. This will result in enhanced resilience and decision making within DRS from the response phase through to the recovery phase of a disruptive incident.

CONCLUSIONS

The scale of a security related incident, whether caused by a deliberate act or of natural causes, is very difficult to judge. We have seen many terror related incidents across the world, which have overwhelmed emergency services due to the size and unexpectedness of an attack, resulting in a reactive approach to response and recovery. Emergency/incident response plans are only one way of proactively responding to an event, however, without competent people using plans they become ineffective.

DRS strive for continuous improvement in security and resilience by being part of and leading emergency exercises in partnership with other key stakeholders, including customers, emergency services and regulators in order to maintain a strong and robust security and resilience culture. This is achieved by testing those personnel who would be utilised in a real-life emergency/incident and contributes to a heightened level of competence maintaining knowledge of current and emerging threats whilst meeting DRS' regulatory requirements.

Physical security at all of our locations is an integral part of what we do as a business. Ensuring that these measures are fit for purpose is critical in maintaining alignment to the NDA mission. However, the measures in place also provide coverage to our commercial activities; for example, security is in place for a £4m ($5.1m) locomotive, up to £10m ($12.7m) worth of goods on an intermodal train and £5m ($6.3m)[1] worth of rail wagons. Add all of these assets to the protection of nuclear material and the fact that all of DRS' personnel are vetted to an appropriate level, provides value for money for the UK taxpayer and a solid platform for further enhancement of an already embedded security and resilience culture.

As detailed in this paper, security is much more than policies and procedures. DRS' in house Security and Resilience department provide very good expertise on all related matters, but a security and resilience culture within an organisation needs to be an integral part of its foundations. As with safety, security in the twenty first century is of paramount importance and training and developing all personnel on security related matters embeds a focussed culture to security and resilience.

In future years, security will continue to be susceptible as the threat evolves, whether this be from a physical terrorist activity or from a cyber-attack. As a business DRS are very much focussed on improving our detection capability to prevent a malicious cyber-attack from taking place.

As nuclear material leaves a licensed site and is taken into the care of DRS, security vulnerabilities are more prominent and as such, emergency/incident response arrangements come into their own. Having these built into the security and resilience culture is key in enabling DRS to continue supporting the NDA mission, whilst always maintaining public safety and public acceptance. Our

[1] *Exchange rate dated 16 May 2019*

other commercial activities are closely aligned to the strategic focus of the business and exercises can be aimed at our nuclear or non-nuclear activities, all critical in promulgating the security and resilience culture.

As a business DRS prides itself on being 'safe, secure, reliable' in all of its operations. Testing personnel, policies and procedures is a vital component of self-auditing and ensuring that good practices are shared, whether from an emergency response or business continuity perspective. Measuring the number of exercises and reporting to Board level provides a level of comfort that DRS are doing all it can in meeting its regulatory requirements, but also promulgating, developing and improving upon its security and resilience culture.

ACKNOWLEDGEMENTS

I would like to acknowledge colleagues from Direct Rail Services Ltd who have supported me in the writing of this paper; Mark W Shiel – Resilience Manager, Julie Mackie – Business Continuity Officer, Yvonne Bannister – Chief Information Security Officer (CISO) and Luke Asbridge – Business Manager.

REFERENCES

1. **IAEA.** Security of nuclear and other radioactive material. *IAEA.* [Online] 25 April 2019. https://www.iaea.org/topics/security-of-nuclear-and-other-radioactive-material.

2. *Integrated Approach Includes Information Security.* **Wood, C.** 2000, Security, pp. 43-44.

3. **Gov.Uk.** About Us NDA. *Gov.Uk.* [Online] 2019. https://www.gov.uk/government/organisations/nuclear-decommissioning-authority/about#mission.

4. *Security-Informed Safety: It It's Not Secure, It's Not Safe.* **Bloomfield, R., Netkachova, K. and Stroud, R.** 2013, Resilient Systems, pp. 17-32.

5. **Kaplan, E.** Rail Security and the Terrorist Threat. *Council on Foreign Relations.* [Online] 8 March 2007. https://www.cfr.org/backgrounder/rail-security-and-terrorist-threat.

6. *Information security culture: A management perpsective.* **Van Niekerk, J.F. and Von Solms, R.** 2009, Computers and Security, p. 1.

7. *Information security management: an approach to combine process certification and product evaluation.* **Eloff, M.M. and S.H., Von Solms.** 2000, Computers and Security, pp. 698-709.

8. **Howsley, R.** *World Institute for Nuclear Security: 4.6 Security Exercises.* Vienna : WINS, 2014.

9. **CPNI.** Critical National Infrastrucuture. *Centre for the Protection of National Infrastructure.* [Online] 2016. https://www.cpni.gov.uk/critical-national-infrastructure-0.

10. **IAEA.** Board of Governors General Conference. *Nuclear Security Plan 2014 - 2017.* [Online] 2013. http://www-ns.iaea.org/downloads/security/nuclear-securityplan2014-.

11. **McAulay, Ron.** *RAIL INDUSTRY TESTS EMERGENCY PLANS.* 24 March 2005.

12. **NIAC.** National Infrastructure Advisory Council (NIAC) Final report and Recommendations: the insider threat to national infrastructures . *US Department of Homeland Security.* [Online] 08 April 2008. http://www.dhs.gov/xlibrary/assets/niac/niac_insider.

13. *Human factors in information security: The insider threat - who can you trust these days?* **Colwill, C.** 2009, Information Security Technical Report, pp. 186-196.

14. **NDA.** Direct Rail Services lifts 6th Golden Whistle Award. *GOV.UK.* [Online] 29 January 2019. https://www.gov.uk/government/news/direct-rail-services-lifts-6th-golden-whistle-award.

15. **Morse, G. and Taberneso, S.** *Learning from Operational Experience Annual Report.* London : RSSB, 2012/13.

16. **RSSB.** Learning from Operational Experience. *RSSB.* [Online] 2017. https://www.rssb.co.uk/risk-analysis-and-safety-reporting/accident-investigation-and-learning/learning-from-operational-experience.

17. **Crosby, P.B.** *Quality is Free: The Art of Making Quality Certain.* New York : New American Library, 1979.

18. **Romeo, C.** 6 ways to develop a security culture from top to bottom. *TechBeacon.* [Online] 2018. https://techbeacon.com/security/6-ways-develop-security-culture-top-bottom.

19. **The White House.** *Nuclear Security Summit 2016 Communique.* Washington DC : s.n., 2016.

20. *The Utility of Table-Top Exercises in Teaching Nuclear Security.* **Hobbs, C., Lentini, L. and Moran, M.** 2016, International Journal of Nuclear Security, p. 1.

21. *Insurance: Lessons from Disasters.* **Schut, J.H.** 1990, Institutional Investor, p. 297.

22. *Business Continuity Planning: A Comphrensive Approach.* **Cerullo, V. and Cerullo, M.J.** 2004, www.ism.journal.com, p. 2.

23. *Quality Is More Than Making a Good Product.* **Takeuchi, H. and Quelch, J.A.** 1983, Harvard Business Review, pp. 139-145.