Risk Informing Security At The U.S. Nuclear Regulatory Commission

Authors

Joe Rivers.
Rivers Security Services, LLC, GERMANTOWN, MD, USA.

Abstract

There have been initiatives at the U.S. Nuclear Regulatory Commission (NRC) to risk-inform security. In order to effectively risk-inform security, a risk structure should be established in order to better understand the overall risk framework, as well as how individual elements of security contribute to the overall risk. Although the staff has offered approaches to establish a structure to risk-inform security, NRC management has chosen to not develop a structured approach. Management cannot see immediate benefit, so chooses to pursue piecemeal approaches that rarely result in any measurable results. However, these activities have cost NRC and the industry significant resources, resulting in few measurable results. This paper will provide insights into the historical efforts to risk-inform security and offer an approach that has a higher likelihood of success.

Background

There have been numerous initiatives at the U.S. Nuclear Regulatory Commission (NRC) to risk-inform security. However, in order to effectively risk-inform security, a risk structure should be established in order to better understand the overall risk framework, as well as how individual elements of security contribute to the overall risk. Although this has been done in the safety arena, it is yet to be done in security. As a result, most of these efforts result in little or no progress to improve security in a risk-informed approach.

Previous and Current Initiatives

The NRC conducted a number of workshops, with the support of Sandia National Laboratories and the INMM, on risk-informing security and Commissioner Apostolakis led a Risk Management Task Force (RMTF) from 2011 to 2012. The workshops identified a number of recommendations to better risk-inform security, with the most consistent one being the need for the security and safety communities to work together to address risk-related issues. The RMTF was tasked with developing a strategic vision and options for adopting a more comprehensive, holistic, risk-informed, performance-based regulatory approach. The task force identified recommendations for the major program areas within the NRC's regulatory program. However, the recommendations tended to be predominantly safety oriented. The limited discussion of security focused on the need to make sure that terminology used in the safety and security disciplines was better understood. In particular, the need was identified to produce a glossary to identify how terminology used in the two disciplines was either similar or different.

There have been a number of activities that addressed some possible improvements in risk informing security. These activities include industry initiatives, internal NRC working groups, rulemaking activities, and international projects. However, the more global ones that were intended to address risk across both security and safety tended to focus on safety, while ignoring security.

The Nuclear power plant industry worked on an effort called the Risk Prioritization Initiative (RPI). This effort focused on developing a process for plants to prioritize projects at a facility based on measures of

risk. The intent was to assess the project's ability to reduce risk, considering safety, security, emergency preparedness, radiation protection, and reliability. Projects that rated highest would be prioritized and initiated earlier than others. The RPI addressed risk related to safety and reliability reasonably well but failed to do so in the other three areas. The effort never succeeded in being implemented.

The Risk Management Regulatory Framework (RMRF) Working Group was established to respond to the recommendations made by the RMTF. This working group initially began work to address the entire scope of the task force recommendations, as well as to develop a policy statement on defense-in-depth. But the scope of the working group's efforts was reduced to just power reactor safety, ignoring security.

The NRC worked for several years to develop a more graded security program for special nuclear material (SNM). Rather than assuming that all uranium and plutonium is equally attractive to a potential adversary, the NRC staff studied how the chemical and physical forms may impact the attractiveness of the SNM. If the SNM is more attractive, the adversary is more likely to attempt to steal the SNM in order to construct an improvised nuclear device (IND). Many such approaches have been investigated over the years, but they generally produce attractiveness approaches that would be too complex to incorporate into a regulatory regime. In the end, an approach was developed that focused on attractiveness being represented by levels of dilution. In principle, the more dilute the SNM, the less attractive the SNM would be to an adversary. This approach was incorporated into a rulemaking, but the rulemaking was canceled by the Commission for "budget reasons" in 2018. The staff has continued to use the technical approach to license facilities on a case-by-case basis since then. On a positive note, the Commission appears to be reconsidering whether the rulemaking should continue to be turned off.

Current initiatives are more narrowly focused, as many were in the past. They include looking at security bounding time, or the amount of time the site would need to defend the facility before there is an effective law enforcement response. Another approach under assessment is to better understand how Flex equipment can support in the mitigation of sabotage consequences. It is not clear whether these initiatives will be implemented, or how much they will better risk-inform security.

A Better Approach?

A better approach would be to understand the overall security risk framework which should be able to yield a better understanding of how each of the individual elements contribute to protecting against the overall risk. The first is the use of modeling and simulation tools to assess the effectiveness of security at individual plants. The second is to develop a general security risk framework that can support decision making at individual facilities and support the NRC in assessing which security risk initiatives have value in pursuing.

The facility level approach has been underway for a number of years. However, it has not been implemented as well as it could have been. Many of the individual facilities modeled and assessed their security systems once or a handful of times. However, these tools provide better insights if they are used on a consistent basis and when the models are continuously updated as there are changes in the security environment. Part of the reason that this has happened is that NRC has been slow to acknowledge the benefits of using these modeling tools. As a result, many of the users have not chosen to use them to their full extent. It would be helpful to both the NRC and the utilities to embrace these tools and make them an integral part of the regulatory process.

The more global level approach has been under development for a number of years but has met substantial resistance from both the NRC and the industry. The NRC questioned the value of supporting the process. What benefit would the NRC see from supporting it? Industry expressed that it was concerned that it would result in a requirement for a security "PRA." But it is not clear what a security "PRA" looks like. What is this global level approach?

The global level approach is underway with the development of a guide by the Physical/Cyber Risk Informing Security Working Group of the Joint Committee on Nuclear Risk Management (JCNRM). JCNRM is a standards organization run by the American Nuclear Society (ANS) and the American Society of Mechanical Engineers (ASME). JCNRM develops standards and guides supporting the use and implementation of risk in the nuclear sector.

The purpose of the working group effort is to provide guidance on the technical application of risk methods to physical and cyber security functions as performed for nuclear facilities in order to support the optimal application of resources. This guidance is intended to provide useful information on risk methodologies, information, and insights such that the effectiveness of physical and cyber security programs can be measured and improved, as appropriate. Pursuant to this, the intent of the working group is to provide insights/guidance on:

(1) risk methods to improve the alignment of the security mission to that of the safety mission of nuclear facilities,

(2) risk methods and approaches to establish risk significance criteria and associated technical basis as applied to nuclear facility security programs,

(3) quantitative and qualitative methods that can be used to assess the effectiveness of security programs, as well as, the significance of security related events originating internally or externally to the facility, and

(4) a means to assess, monitor, and observe on-going performance trends of security functions through risk-informed facility specific performance indicators.

The working group will be completing the guide in the near future. At the same time, the working group leadership will engage with stakeholders to ensure that they better understand the effort and to gain their support. Upon completion of the guide, topical areas will be identified to develop more specific guidance on risk-informing security elements and systems. The working group leadership will work with stakeholders to identify the priority of topical areas to focus on. The prioritization will be based on the contribution to overall risk reduction of the topical areasecurity element or dydtem covered by the topical area, along with the likelihood of successfully finding an approach to risk-inform the security element or system.

Conclusion

The global approach to risk informing security discussed in this paper that is being developed by the JCNRM working group has a high likelihood of success. Its success is a product of the successful integration of safety and security risk professionals working together. It will also attempt to assess security program elements' contribution to addressing risk and the likelihood of developing an approach as part of the process.