Evaluating the Effectiveness of Insider Threat Mitigation Preventive Measures

John Landers, Ph.D., Oak Ridge National Laboratory

Sondra Spence, Sandia National Laboratories

Bill McGlennon, Sellafield Ltd.

Eric Gosset, Commissariat à l'énergie atomique

Baleigh Morgan, Nuclear Cybersecurity Specialist, Idaho National Laboratory

Abstract

Malicious insider threats are real and persistent in the nuclear industry and have existed since the industry's inception. Fortunately, actual malicious insider actions appear to be rare events. The assumption is that effective insider threat mitigation programs (ITMPs) screen out applicants exhibiting behaviors predictive of future threats, deter potential malicious insiders, and facilitate detection and effective responses to known malicious actions. The low base rate for malicious insider behavior, however, could also explain why these behaviors are rare without having to invoke the ITMP as explanatory. Although there are defined methods to evaluate the effectiveness of ITMP protection measures (i.e., detecting and responding to threat acts), assessing the effectiveness of preventive measures (i.e., deterring those considering using their access, authority, and knowledge as insiders from committing malevolent acts, or determining whether all people who are potential insiders have been screened out) has been elusive. If we assume that these programs and measures reduce the risk from insider threats, methods can be developed to evaluate how effectively the preventive aspects of programs and measures are being implemented. For example, if a trustworthiness program includes background checks to identify personnel with previous criminal convictions, a random sampling of previously completed background checks, or performing independent checks, can verify whether the program is working by comparing results. Alternatively, a fake applicant with a criminal conviction could be inserted into the system to determine if the conviction is identified. Current performance evaluation of ITMPs must evolve beyond compliance to address the evolving insider threat because data from this process can be used to invest in program components that are the most effective and upgrades can be made to those that fail to meet expectations. This panel brings together experts from various backgrounds to propose methods for determining the effectiveness of ITMP preventive measures.

Introduction

Malicious insider threats have been a persistent issue since the inception of the nuclear industry. Insider Threat Mitigation Programs (ITMPs) serve to screen applicants exhibiting behaviors predictive of future threats, deter potential malicious insiders, and facilitate detection and effective responses to known malicious actions. Despite the defined methods for evaluating the effectiveness of ITMPs' protection measures, the assessment of preventive measures has been elusive. This paper brings together the views of experts to propose methodologies for determining the effectiveness of ITMP preventive measures and provides self-assessment questions for performance assurance practices and implementation of changes in insider threat mitigation.

Why and What to Measure

ITMPs, based on a graded approach consistent with Design Basis Threat (DBT), aim to mitigate the threat by including several potential components. Each component is embedded with detection, delay, and response features. The ITMPs' effectiveness and compliance are measured against this threat, thus providing a means for assessing risk mitigation of identified threats and highlighting potential areas of system improvement. Components of ITMP to be assessed include facility planning/management/administrative procedures, personnel security/polygraph, physical protection, nuclear material accounting and control (NMAC), cybersecurity, security culture, human reliability program/behavior observation program/fitness for duty/access control, employee assistance program/mental health program, and personnel training.

How to Measure

Assessment requires a reliable, valid, and standardized approach, with performance assessed against a defined threat. Risk is assumed and measured via risk mitigation compliance and effectiveness through performance assurance methods. This includes prescriptive methods such as checklists against requirements and random sampling of processes. Performance methods can range from simple tests of a sensor to tactical exercises involving adversaries. Ideally, assessment should be under normal conditions (naturalistic) and under simulated conditions (artificial), with maximum realism as the target.

Self-Assessment Questions for Performance Assurance Practices

The self-assessment of current performance assurance practices and the implementation of changes within an organization can begin with introspection at various levels, including human factors, organizational culture, and the measurability of aberrant behaviors.

Human Factors:

1. How effectively are we measuring human performance in recognizing aberrant behavior, considering its nuanced nature?

2. How are we accounting for cultural differences that might impact the effectiveness of our insider threat mitigation measures and their performance testing?

3. What are the key metrics or indicators we are currently using to measure the efficacy of policies and procedures designed to mitigate insider threats?

Organizational Culture:

4. How are we fostering a culture that encourages reporting aberrant behavior without promoting suspicion and distrust?

5. How does the fear of false positives or false negatives influence our design and implementation of insider threat mitigation measures?

6. What are the significant challenges we face in accurately performance testing our insider threat mitigation measures?

Aberrant Behavior Measurement:

7. How are we ensuring the reliability and validity of tests measuring the effectiveness of our insider threat mitigation measures?

8. Are there any potential biases that could affect the recognition and reporting of aberrant behavior? How are we controlling for these biases during performance testing?

9. Considering the subjective nature of aberrant behavior perception, how are we standardizing its measurement across different teams or departments?

Emerging Considerations:

10. How have technological advancements impacted our performance testing of insider threat mitigation measures? Are there specific technologies that have improved our process?

11. How do we balance privacy rights with security needs in the implementation and testing of our insider threat mitigation measures?

12. What role do our employee training and awareness programs play in mitigating insider threats? How are we measuring their effectiveness?

13. Are we exploring or employing any innovative or unconventional methods for performance testing of insider threat mitigation measures?

14. How do we test and measure the effectiveness of our response to reported aberrant behavior?

15. Are there any case studies where our performance testing has significantly improved our ability to mitigate insider threats?

16. What are the foreseeable challenges or developments in the field of insider threat mitigation and its performance testing in the next 5-10 years?

Preventive Measures and Performance Testing Scenarios

The performance of preventive measures can be tested through diverse scenarios. Examples include checking the system's ability to challenge authority when a manager tries to access data without the need-to-know, quality assurance checks on incidents to ensure proper information sharing, inserting derogatory information into fictional applications to test personnel security screening, and testing the capacity of peers to recognize and report progressive but innocuous aberrant behaviors for early intervention. These scenarios provide insights into the challenges posed during testing and how to mitigate these challenges. Findings from these tests can lead to improvements in the ITMP and help in creating additional test scenarios.

When and Who Measures

The process of assessing the effectiveness of Insider Threat Mitigation Programs (ITMPs) should ideally be an ongoing activity that can be categorized into four primary phases:

1. Planning and Management: *This phase involves the formulation of ITMP strategies, identifying potential threats, deciding on appropriate preventive measures, and establishing clear procedures for handling potential threats. This planning process should be regularly revisited and updated to account for changes in potential threats and security technology advancements.*

2. Preparation and Analysis: *This is the phase in which the actual methods for measuring the effectiveness of the ITMP are developed and put in place. These might include compliance assessments, performance testing, and more. As with the planning phase, the preparation phase is not a one-time event but should be regularly updated to reflect current best practices and threat landscapes.*

3. Reporting and Oversight: *Regular reports on the effectiveness of the ITMP are crucial to maintaining security. These reports should cover both the results of the measurement and evaluation procedures and any actual incidents of insider threats. They should be reviewed by senior*

management and security personnel to ensure that the ITMP is functioning effectively and to identify any necessary adjustments or improvements.

4. Quality Assurance: *Regular audits and reviews should be conducted to ensure that the ITMP is operating as intended and that all components are functioning correctly. These audits can be carried out by internal staff, or they may be conducted by independent third parties for additional objectivity.*

As for who should be responsible for these measurements, this can vary based on the organization's structure and resources. Generally, the responsibility should fall on a dedicated security team, trained in the specific nuances of ITMPs. This could include internal security personnel or independent third-party reviewers. The advantage of using internal personnel is their understanding of the organization's specific context and environment. Third-party reviewers, on the other hand, bring an external perspective and can help identify issues that may be overlooked by internal staff due to familiarity with the organization's workings.

Regardless of who conducts the assessments, it is vital to have clear communication channels so that the information can be shared with key decision-makers and stakeholders. This ensures that findings from the assessment lead to actionable changes, enhancing the overall effectiveness of the ITMP.

Recommendations, Summary, and Conclusion

Insider threats pose a complex and ongoing challenge for the nuclear industry, requiring a sophisticated and responsive set of mitigation measures. The effectiveness of these measures is predicated on a robust, multi-faceted Insider Threat Mitigation Program (ITMP) that must be continually assessed, refined, and strengthened.

Firstly, when considering the insider threat, vulnerability assessment must account for additional complexities not traditionally found when detecting, delaying, and responding to external threats. The malicious insider, often having a deep understanding of the system, can exploit opportunities not readily visible to external observers. They may also exhibit alarm signs, such as aberrant behavioral indicators, which necessitate a careful and nuanced approach to detection.

Our panel emphasizes the need for a robust performance assurance process that tests the ITMP as it is designed to operate, as well as under scenarios where systems fail to function as intended. This process allows us to examine the depth of defense built into the ITMP through various components and scrutinizes their integration and interaction under different scenarios. Such rigorous testing allows for the identification of weak points in the system, providing the opportunity to make necessary improvements and upgrades.

A successful performance assurance system requires both prescriptive and performance-based methodologies. The former ensures compliance with established procedures and regulations, while the latter tests the system's overall effectiveness in real-world scenarios. The cross-validation of these two methodologies is key for confidence in risk mitigation estimations.

In the context of continuous improvement, the feedback from performance assurance assessments can inform ITMP design adjustments. Prioritizing components that provide greater risk mitigation in these assessments can lead to resource allocation that maximizes the effectiveness of the ITMP. This continual refinement is a necessity given the evolving nature of insider threats and the increasing complexity of systems at risk.

Lastly, the question of who performs these measurements is of considerable importance. The responsibility should ideally be vested in a dedicated security team well-versed in ITMP nuances, whether they are internal security personnel or an independent third-party reviewer. This team must maintain clear communication channels to ensure findings from assessments lead to actionable changes, thus enhancing the overall ITMP effectiveness.

Acknowledge the Complexity of Insider Threats

Establish Robust Performance Assurance Process

Implement Both Prescriptive and Performance-Based Methodologies

Employ Cross-Validation of Assessment Methods

Prioritize Components in ITMP Design Adjustments

Designate a Dedicated Security Team for ITMP Assessments

Maintain Clear Communication Channels for Actionable Changes

In conclusion, a proactive, comprehensive, and continuously improving ITMP, combined with a robust performance assurance program, forms the cornerstone of effective insider threat mitigation in the nuclear industry. This panel discussion has sought to highlight the critical considerations in achieving this, laying out a roadmap for the evaluation and enhancement of ITMP preventive measures. As the threat landscape evolves, so too must our response, with regular and comprehensive assessments serving as the touchstone for continued security and risk mitigation.

References

IAEA. (2019). Nuclear security assessment methodologies for regulated facilities. IAEA. Retrieved August 29, 2022, from https://www.iaea.org/publications/13416/nuclear-security-assessment-methodologies-for-regulated-facilities

INS. (2020). Roadmap: Facility Implementation of an Insider Threat Mitigation Program. INS. IM Release number: LLNL-TM-829505.

WINS (2020). 3.8 countering violent extremism and insider threats in the nuclear sector. WINS. Retrieved August 29, 2022, from https://www.wins.org/document/3-8-countering-violent-extremism-and-insider-threats-in-the-nuclear-sector-mitigation-strategies/

WINS (2021). 3.4 managing insider threats in the nuclear industry. WINS. Retrieved August 29, 2022, from https://www.wins.org/document/3-4-managing-insider-threats-in-the-nuclear-industry/