Proceedings of the INMM Joint Annual Meeting
May 22-26, 2023

OPERATIONALIZING INSIDER THREAT POTENTIAL AND RISK-SIGNIFICANT INSIDERS TO ENHANCE INSIDER THREAT DETECTION AND MITIGATION

Colton Heffington, Adam D. Williams, Shannon Abbott, Christopher Faucett, and Sondra Spence
Sandia National Laboratories*
Albuquerque, NM, USA, cpheffi@sandia.gov

William Charlton
Nuclear Engineering Teaching Laboratory
University of Texas, TX, USA

Katherine Holt
Office of International Nuclear Security, National Nuclear Security Administration,
Washington, DC, USA

Melinda Lane
Lawrence Livermore National Laboratory
Livermore, CA, USA

Recent trends in insider threat for critical facilities have shifted focus toward determining the potential for a successful insider act. Consider, for example, Homeland Security's Cyber and Infrastructure Security Agency (DHS/CISA) 2020 Insider Threat Mitigation Guide, which defines insider threat as "the *potential* for an insider to use access or special understanding of an organization to harm that organization." This shift suggests a range of drivers of "the potential for an insider" to act—expanding beyond traditional insider threat mitigation programs that heavily emphasize preventative and protective strategies to deter the behavior of bad actors.

Ongoing research at Sandia National Laboratories and the University of Texas—in support of international efforts to improve insider threat mitigation for nuclear facilities (e.g., International Atomic Energy Agency INFCIRC/908) for the United States National Nuclear Security Administration's Office of International Security (NNSA/INS)—investigates the impact of shifting insider threat detection and mitigation (ITDM) from a sole focus on identifying and deterring malevolent individuals behaviors toward including collective workplace behaviors observed in nuclear facilities. This new approach to ITDM builds on continuing research that invokes artificial neural networks to capture, collate, and analyze disparate data signals to quantitatively describe operational workplace patterns in search of identifying risk significant insiders. Combining key concepts from organization science and nuclear safety, this paper offers a revised approach to insider threat mitigation based on *risk significance*, a measure of the capability that an individual possesses to successfully carry out an insider plot. We argue that individual-level deviations from expected workplace behaviors may be indicative of increasing risk significance. We further propose a series of experiments and discuss whether artificial neural networks can aid us in generating measures of expected workplace behavior and thus also capture risk significant deviations.

* SAND2023-03216O, Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

INTRODUCTION

Recent trends in insider threat for critical facilities have shifted focus in determining the potential for a successful insider act. For example, in their 2020 Insider Threat Mitigation Guide, the Department of Homeland Security's Cyber and Infrastructure Security Agency (DHS/CISA) defines insider threat as "the *potential* for an insider to use access or special understanding of an organization to harm that organization" (emphasis added). Shifting to focus on "the potential for an insider" to act suggests a different set of drivers—hypothetically expanding beyond traditional insider threat mitigation programs that heavily emphasize preventative and protective strategies to deter malevolent behaviors of individuals.

Building on best practices exhibited in the nuclear industry (e.g., from the United States Nuclear Regulatory Commission [1]) and lessons learned from other industries (e.g., the casino industry [2]), there seems to be a benefit from invoking an empirical and data-driven approach to counter insider threats. One key challenge for such an approach is the ability to distinguish between malicious intent and natural organizational evolution—as both may present as anomalies from expected behaviors in the workplace. Yet, such deviations from expected patterns may form the foundation for defining—and measuring—the *capability* of an insider to successfully execute a malicious act. We refer to this capability as *risk significance*.

In support of international efforts to improve insider threat mitigation for nuclear facilities [3], current research at Sandia National Laboratories is investigating similar approaches to insider threat mitigation. More specifically, under sponsorship from the United States National Nuclear Security Administration's Office of International Security (NNSA/INS), Sandia is exploring the impact of shifting insider threat detection and mitigation (ITDM) from solely focusing on identifying and deterring malevolent individual behaviors toward incorporating workplace behaviors observed in nuclear facilities. Our first set of efforts demonstrated that we can generate empirical expectations around "expected" behavior at the individual-level based on the individual's group identity within the facility (i.e., graduate students, technical staff, maintenance, etc.) and use neural networks to detect significant deviations based on insider threat behavior [4].

Based on this initial set of findings, we offer a revised theoretical framework, a new set of experiments, and findings that advance our approach to ITDM. This approach introduces concepts from the field of nuclear safety into our discussion on nuclear security and draws on new research [11]. We argue that every member of the workforce, and indeed every behavior in the workplace, can be characterized in terms of risk significance. A risk significant insider is one that has the capacity to execute some element of an insider attack, whether it be sabotage or theft. We argue that a data-driven method to measuring risk significance will help increase the probability of detection in case of a genuine insider threat and enhance the validity of risk perception in the minds of security personnel, managers, and administrators who are tasked with estimating risk in advance of a genuine insider effort.

This paper proceeds by summarizing our previous work to provide theoretical and empirical context. We then detail our new theoretical approach and outline proposed experiments.

PREVIOUS RESEARCH: COLLECTIVE BEHAVIORS & WORKPLACE RHYTHYMS

Our initial theory relied heavily on concepts derived from the organizational science and safety literature, including Rasmussen [7]. We argued that observable patterns resulting from everyday behavior can be measured to create expectations around individual-level behavior in a given setting. Such an approach is used regularly in the study of safety to identify the gaps in various processes that may represent safety risks. In the realm of insider threat, we argued that deviations from expectations represented insider threat potential (i.e., higher risk actions in the safety parlance). Our goal was initially to use data to define acceptable bounds of behavior within a secure facility because, of course, not all deviations represent a genuine increase in insider threat potential. Instead, we focused on large-scale deviations of expected behavior associated with hypothetical insider plots (e.g., unauthorized attempts to open a closet housing security systems).

Sandia's initial empirical efforts consisted of installing a commercially available artificial neural network (ANN) at the University of Texas' Nuclear Engineering Teaching Laboratory (NETL)—which hosts a TRIGA MARK II research reactor. The research focused on the ability of this ANN to "learn" the operational patterns of NETL and examine the software's ability to detect "off-normal" personnel activities. The general hypothesis indicated that larger deviations from expected behaviors (or larger anomalies) would indicate elevated risk levels for suspected regions of the facility. By logical extension, this research sought to ascertain the extent to which leveraging a better understanding of workplace dynamics—also called operational patterns of a facility—improves the ability to identify, detect, and forecast insider threat activities.

Table 1. Summary descriptions of data categories for Sandia's ANN-based research for insider threat mitigation

Category	Description	Implication
Single access point (SAP)	All access control data was organized by sensor location in the facility, date and time of allowed access, and then by identity used for access	Allowed for observation of patterns of accesses in time including bounds for when particular accesses are expected to occur for all individuals as well as for specific individuals
Time-sequenced, multiple access points (TS/MAP)	All access control data was organized by identity used for access, by date and time of allowed access, and then by location in the facility	Allowed for observation of patterns of access by individuals including bounds for when particular individuals would be expected to complete a sequence of access to different locations
Time of access by personnel type	All access control data was organized by access point, date and time of allowed access and then by grouping the identity used for access into a personnel type	Allowed for observation of pattern differences between personnel groups: Facilities, Administrative, Faculty, Research Staff, Operations, Graduate Student, Undergraduate Student

More specifically, this research emphasized the ability for ANN-type solutions to derive operational patterns from *existing* data collectors. For the NETL research, early data was collected from door access readers and intrusion alarm systems (and future experiments will include area radiation monitors and personnel radiation detection portals). The collected data were organized for analysis to observe any trends in the bounds of the NETL operational patterns. The data categories evaluated are summarized in Table 1.

Even with the NETL research and education mission and the diversity of personnel, operational rhythms of the facility show a regular set of patterns. Consider analysis of the data associated with first entry to the reactor control room, illustrated as a frequency distribution of the first allowed access to the NETL reactor control room versus the time of access (Figure 1). As shown, there are clear bounds on normal or expected times of first entry to the reactor control room on all working days—and, in this case, the same results occur regardless of whether weekends and holidays are included. By virtue of timing within early phases of this research, data was collected before and after COVID-19 protocols restricted normal operations—and potentially changing operational patterns. Yet, Figure 1 showcases very similar bounds and profiles of first entry into the NETL control room.

Though a representative result, Figure 1 showed us that the ANN can establish bounds on operational patterns as a baseline for analyzing deviations in behavior outside of these bounds. Since the bounds to operation became smaller overtime and not larger, the ANN did not flag any of these changes as off normal behaviors, thus our current research is needed.

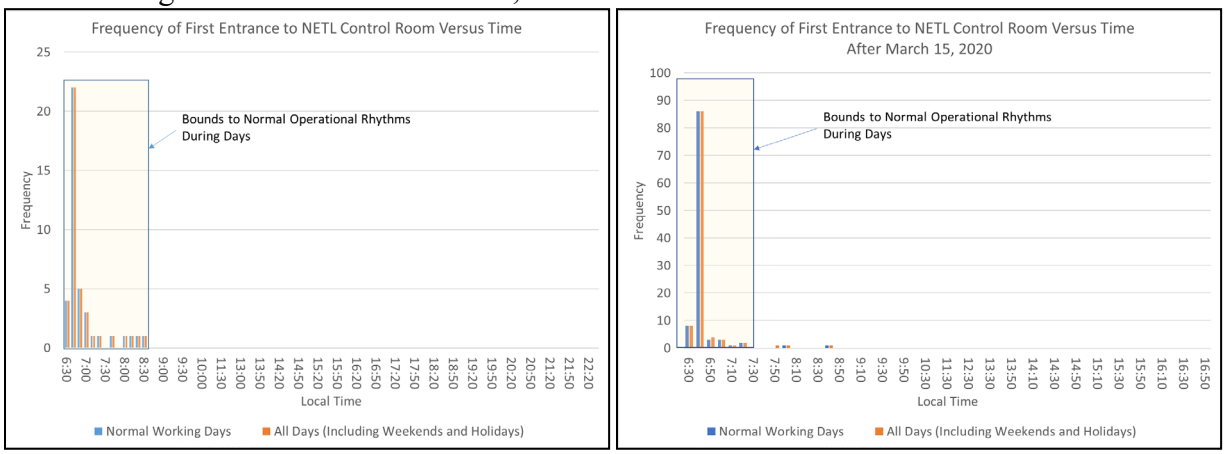

Figure 1. Frequency distribution showing time of first entrance to NETL control room separated by working days only and all days for (A) before COVID-19 lockdowns and (B) after initial COVID-19 lockdowns.

Similarly, Figure 2 shows early results from evaluating the time of first entry to the NETL by personnel group. As illustrated, each personnel group has specific patterns:

- *administrative* and *operational* personnel have very tightly bounded patterns in time
- *faculty*, *undergraduate students*, and *graduate students* have more loosely bounded patterns in time

In contrast to the results in Figure 1, COVID-19 lockdown protocols had a direct impact on these distributions, with a noted severe decrease in activity by graduate students, faculty, and for undergraduate students (which has decreased to zero accesses since March 15, 2020). The ANN is also able to identify deviations in patterns *both* from expected personnel group patterns and expected individual activities when those deviations lead to a new access.

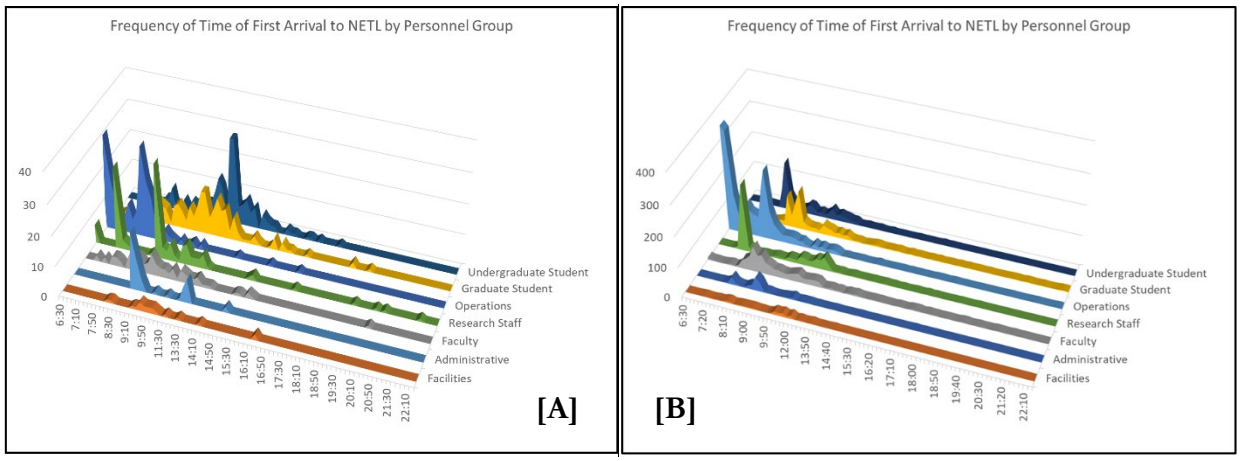

Figure 2. Frequency distribution showing time of first entrance to NETL separated by personnel group for (A) before COVID-19 lockdowns and (B) after initial COVID-19 lockdowns.

For a more detailed exploration of this current research, please see [5]. These initial empirical analyses demonstrated that it was possible to use data gathered by a neural network to both define organizational rhythms and identify deviations from that organizational rhythm. We now advance a revised, more comprehensive theory based on the assessment of insider risk significance.

A REVISED FRAMEWORK FOR INSIDER RISK SIGNIFICANCE

Many practical models of insider threat focus on identifying insider threats and using preventive and protective measures to stop inside insider plots from coming to fruition [8]. New practical approaches also emphasize the ability to identify insider threats before they occur based on IT signals and psychometric test results [10]. Other approaches argue that a security culture built around mutual respect and *positive deterrence* can stymie insider plots [14]. A developing theoretical debate addresses the different pathways that insiders take in their radicalization [12][13]. Regardless of the path an insider takes or the signals that we use to detect insider plots, much of the literature agrees that insiders provide evidence of their impending plots before they execute their attack (e.g., The Fort Hood terrorist attack) [15]. We share this assumption, though our theory does not rely on it. In other words, we seek to build a flexible theoretical approach that incorporates concepts like “preventive and protective measures”. We further maintain an agnostic view on insider pathways and the use of different signals to measure insider risk significance.

Beginning with these assumptions, we offer a theoretical framework for insider threat built around *risk significance*. We borrow the term risk significance from the safety literature, as a concept that is used to characterize the estimated frequency of an adverse event and the degree of consequence; any possible accident that exceeds a policy-determined limit is definitionally *risk significant*. We use this same concept to characterize the risk associated with any one person in a nuclear facility, which is best conceptualized as a time-variant continuous variable. We consider individuals to be specifically highly risk significant if they currently possess the ability to successfully execute an insider plot. In other words, this variable inherently possesses a critical threshold that varies by both individual and facility. Individuals that cross the threshold of

capability are risk significant by induction. Note that this individual-level measure is partly a function of facility policy and security systems too [11]. An individual with low levels of access and knowledge could still be risk significant if security procedures in a given facility are poor or routinely violated.

Insiders who carry out successful attacks (e.g., the above-mentioned Hasan Nidal at Fort Hood) are, by definition, risk significant insiders. Every individual possesses some combination of access, authority, and knowledge that determines their risk significance status. A junior member of the human resources staff with no access to sensitive areas of a nuclear facility is probably not risk significant unless they can manipulate the facility's physical security systems to a considerable degree. A facility manager who has near-universal access and authority over nearly all personnel is probably risk significant. While it's possible to generate a rough guess about the level of risk significance that any one member of the workforce, we obviously cannot know *a priori* what that value is for everyone. We argue below that measures of workplace rhythms gathered over time using facility sensors and artificial neural networks can increase the validity of our measures of risk significance at the individual-level both before and during an actual insider attack/theft.

The goals of any ITDM program, then, must include ongoing efforts to minimize the total number of risk significant insiders to an acceptable level determined by regulatory policy. We assume that reducing the number of risk significant insiders to zero is the goal of regulatory policy. Ideally, any IDTM program would detect anomalies at the individual (insider)-level well in advance of any attack or theft but valid point prediction of insiders before an attack is a difficult empirical problem to address and is likely impossible to address completely (i.e., with a high degree of accuracy and a low number of false positives). In sum, we must use policies to minimize the number of individuals who have the capacity to carry out an attack, and detection capabilities play a pivotal role in that process.

TYPE 1 AND TYPE 2 DETECTION

To better understand the role of *detection* in our approach to ITDM, we use the terms Type I detection and Type II detection. Type I detection refers to the ability of current policies and systems to detect genuine insider threats *before* any physical sabotage or theft effort takes place allowing the insider to gain control of sensitive material, while Type II detection refers to the ability of policies and systems to detect an insider *after* they have already acquired material (or committed a physical act of sabotage in the case of an attack).

The level of risk significance possessed at the individual-level by any one person is definitionally related to both types of detection—a truly risk significant insider can steal material while avoiding Type I or Type II detection. Our goal here, both theoretically and empirically, is to establish a set of systems and/or policies that can lower the risk significance of the entire workforce simultaneously and increase the odds of both Type I and Type II detection in the case of a genuine insider effort.

To aid in this detection process, we introduce expectations about behavior in the workplace. By measuring collective behavior and organizational rhythms within the workplace, we can define expected behavior at the individual-level for any member of the workforce with common-sense

bounds. In turn, we can define serious departures from expected behavior as those that *increase* risk significant behavior. The behavior we focus on here is that which occurs in physical space (as opposed to cyberspace or the behavior that occurs away from the facility). Therefore, expected behavior might include the time in which an employee clocks in or out, the locations they travel to, and the sensitive areas they attempt to access at particular times. As demonstrated in our previous research, much of an individual's expected behavior is driven by their role and/or the groups they belong to (not their individual habits, like the timing of work breaks). We assume that significant deviations from expected behavior increase the risk significance of an individual.

Note above that we said risk significance likely varies in most facilities based on role. By drawing expectations of acceptable behavior from an individual's role, our approach partly accounts for or *controls for* the reality that some workers innately possess a high level of risk significance as a function of their job title. Consider the following vignette that exemplifies this logic:

Jane is an advanced undergraduate student who contributes to ongoing research at a reactor as part of her degree program. Jane, who is considering pursuing a graduate degree, is invited by her academic advisor, who works at the reactor, to observe a graduate research project. This graduate research occurs in a nearby non-sensitive area of the facility, but it is not in an area that Jane has worked in before. Over a period of several weeks, Jane visits the other research group for less than an hour on several occasions, but neither Jane nor her professor alert facility security of this change. This research group meets during Jane's normal hours, so sensors do not register a new time pattern for Jane. However, her movements in new areas of the facility are registered by various physical sensors, and this appears to be a deviation from her expected work activities as an undergraduate student.

In this case, Jane's risk significance has increased, probably not by a large magnitude and not enough to make her fully risk significant, but a combination of her behavior and a failure of policy (security was not alerted by her temporary change in role) is measurable. Again, we assume that more significant deviations from expected behavior increase the risk significance of any individual. By measuring Jane's expected behavior and subsequent deviations, our approach will have measured an increase in risk significance that would not be captured by psychometric tests or cybersecurity monitoring systems. More importantly, our approach should increase the chances of *both* Type I and Type II detection in the case where Jane represents a genuine threat. This is because artificial neural networks ingesting data based on physical movements (tied to an individual) can register significant deviations from expected behavior in (near) real-time. Therefore, ANN systems could register both plotting and scouting movements, as well as sudden drastic deviations associated with, say, the theft of material.

IMPROVING RISK PERCEPTIONS

All security personnel in sensitive facilities are tasked with assessing the risks of insider threat attached to members of the workforce. Whether security analysts do this implicitly (i.e., "trust their gut") or use more objective, systematic tools (e.g., a cybersecurity suite that flags unusual cyberactivity regardless of user) to create spreadsheet data, these analysts possess a *risk perception* related to every person in a facility. Risk perceptions reflect current estimates of *risk*

significance, which in many cases will not be perfectly valid due to incomplete information or measurement error. The goal of any ITDM system or tool is to help close the gap between risk perception and risk significance. Estimating expected workplace behavior and measuring deviations from these expectations helps inform our risk perceptions, and in the case of genuine insider threats, increases the odds of a Type I or Type II detection. In the following section, we outline a series of experiments that test this contention and describe the results.

RESEARCH DESIGN AND PROPOSED EXPERIMENTS

To test our initial claims related to workplace rhythms and expected behavior, we installed several different commercially available software products at NETL. These products used artificial neural networks to measure "normal" operational behaviors at the facility, and we demonstrated that data collected by badge readers, balanced magnetic switches, and area motion sensors could detect efforts to access a closet where security hardware is stored and unauthorized attempts to access the reactor bay, but failed to recognize surveillance of the fuel storage area and authorized efforts to access a secure area using stolen credentials (i.e. the ANNs did not succeed in Type I detection when simulated insiders "scouted" the fuel storage area). In sum, we tested the ANNs' Type I detection capabilities, and attempted to simulate insider attacks that varied between mild levels of risk significance (the simulated insider did not use foreknowledge of sensor locations to avoid detection) to more severe levels of risk significance (the simulated insider stole another user's physical credentials). In the current wave of experiments, we plan to vary the level of risk significance in one set of tests and design new tests around Type II detection as well.

The ANNs used for the planned experiments described here were previously trained on data from badge readers, balanced magnetic switches, and area motion sensors in both single-access-point operational patterns (cases where access data was organized by the access point, time, and identity of the individual), as well as time-sequenced multiple-access point operational patterns. In these more complex instances, the ANN was trained to expect an individual to complete some process during specific time bounds (e.g., traverse a hallway this is bookended by sensors gathering data). In this manner, we can generate data that tells us when personnel arrive, where they go, when they leave, and how long they generally take to complete certain tasks in physical space. We can also generate expectations about their typical behavior—and ideally capture large deviations that may be indicative of security threats. Each ANN product ingests data from sensors and is programmed to generate an alert when a significant deviation is detected. The goal in each experimental scenario is for the ANNs to trigger this alert during a simulated insider threat event. To improve our results relative to the first wave of experiments, we have installed new ANN software and trained these products to detect anomalies consistent with our empirical expectations. As of this writing, we are still gathering data for the second wave of experiments to be integrated into future drafts of this paper.

All data collected for all experiments has been anonymized. Moreover, we use professional role and group membership to determine expected behavior. This means that calculations of an individual's expected behavior are not based only on their actions but entirely on the actions of the group they belong to. That is, the ANN software would not track an individual taking a break from work *unless* they entered a sensitive area that is unexpected given their professional role.

While we lose data fidelity with this group-based approach, we also necessarily preserve key elements of employee privacy, such that the ANNs are not generating individual-level expectations using individual-level data.

SUMMARY OF PLANNED EXPERIMENTS

Varying Insider Risk Significance in Type I Detection Experiments

We developed three "baseline" experimental scenarios that can be replicated with the simulated insider expressing varying levels of risk significance (i.e., knowledge, access, and authority).

- In the first scenario, an individual approached a locked closet where security hardware (servers) is stored and attempted to access the closet.
- In the second scenario, a simulated insider approached the reactor bay and attempted to enter the bay itself.
- In the third scenario, a simulated insider approached the fuel storage area, loitered in the area, and tested the physical sensors in the area as a method of scouting.

To see whether the ANNs were able to achieve Type I detection in these scenarios where the risk significance of the insider varied, we plan to rerun these baseline scenarios with different insiders. First, we intend to run these experiments assuming the insider had no or limited information about the location and function of each sensor gathering and sending data to the ANNs. These scenarios represent cases of limited risk significance. Then, we will run the same experiments with a knowledgeable insider who knows the location of each relevant sensor and knows how the sensors gather data. In these scenarios, the higher risk insider will attempt to physically evade the sensors. The scenarios represent the high-risk significance scenarios. Again, we expect the ANNs to trigger alerts in all cases.

Type II Detection Experiments

Next, we will run our baseline experimental scenarios and assume in each case that the simulated insider was successful in the "phase one" element of the plot described directly above. That is, we will assume that the insider gained access to the security closet or gained access to the reactor bay or successfully scouted the fuel storage area. We will impose circumstances that would allow the simulated insider to gain access to sensitive material. From there, we will continue the scenario with the simulated insider in each case creating and navigating an escape route from the facility. While the level of risk significance does not vary in these scenarios, as we run them all with a "naïve" insider, this is our first effort to learn whether the ANNs can achieve Type II detection, assuming our insider has the capability to avoid Type I detection.

CONCLUSION AND IMPLICATIONS

Our approach here is designed to be flexible and accommodate other popular approaches to ITDM, while demonstrating novel theoretical and technological progress. For example, our approach speaks to detecting anomalies in physical space—and could easily be integrated with other practical solutions that rely on IT signals or tests and evaluations (e.g., psychometrics) used in some human reliability programs. Incorp

An ITDM approach built around risk significance—and measures of deviations from expected behavior—is justified for several reasons. First, the concept of insider risk significance can be directly and clearly described with data-driven approaches that can reduce bias resulting from insider threat mitigating heavily focused on individual psychological stressors/indicators. In other words, our approach will increase the validity of risk perceptions by relying on more objective data. Second, the concept of risk significance provides a conceptual framework to directly incorporate data *already being collected* at nuclear facilities—often for occupational safety and quality assurance reasons—for improving ITDM. In this manner, insider potential-based approaches can avoid the challenges when behavioral reporting systems were in place, obvious signs were dismissed, rationalized, or disregarded on the grounds of existing personal or professional relationships. Again, this will allow our risk perceptions to match risk significance more closely. Lastly, introducing a risk significance-based approach can help streamline the process for investigating anomalous behaviors and, potentially, anticipate which future deviations in workplace patterns most likely indicate malicious intent (versus those resulting from changing overall operational dynamics).

REFERENCES

[1] United States Nuclear Regulatory Commission (2009). "Regulatory Guide 5.77: Insider Threat Program," <https://www.nrc.gov/docs/ML1521/ML15219A609.pdf>.

[2] Bunn, Matthew and Kathryn Glynn (2017) "Preventing Insider Theft: Lessons From the Casino and Pharmaceutical Industries." In Insider Threats, Ithaca, NY: Cornell University Press, pp. 121-144.

[3] International Atomic Energy Agency (2017). "Information Circular 908—Joint Statement on Mitigating Insider Threats," < https://www.iaea.org/sites/default/files/publications/documents/infcircs/2017/infcirc908.pdf>.

[4] Williams, Adam D., Shannon Abbott, Sondra Spence, Nathan Shoman and William S. Charlton (2021) "Phase II Results from an Artificial Neural Network-Based Approach to Insider Threat Detection & Mitigation," Proceedings of the Institute of the Nuclear Materials Management 62nd Annual Meeting.

[5] Williams, Adam D., Shannon N. Abbott, Nathan Shoman, and William S. Charlton (2021) "Results From Invoking Artificial Neural Networks to Measure Insider Threat Detection & Mitigation," *Digital Threats*, 3(1), Article 3, https://doi.org/10.1145/3457909.

[6] Cyert, R. and J. March (1963) A Behavioral Theory of the Firm, Englewood Cliffs, NJ: Prentice-Hall.

[7] Rasmussen, Jens (1997) "Risk management in a dynamic society: A modelling problem" *Safety Science* 27(2), pp. 183–213. https://doi.org/10.1016/S0925-7535(97)00052-0.

[8] Preventive and Protective Measures Against Insider Threats. (2020). IAEA Nuclear Security Series. No. 8-G(Rev. 1).

[9] Hobbs, Christoper and Matthew Moran (2015). "Insider Threats: An Educational Handbook of Nuclear and Non-Nuclear Case Studies," King's College London.

[10] Kandias, Miltiadis, Alexios Mylonas, Nikos Virvilis, Marianthi Theoharidou, and Dimitris Gritzalis (2010). "An Insider Threat Prediction Model." *Trust, Privacy, and Security in Digital Business* 7, 26-37.

[11] Faucett, Christopher Anthony. 2022. Development of a Conceptual Multi-Insider Risk Model for Nuclear Facilities. Dissertation. Texas A&M University.

[12] Lenzenweger, Mark F., and Eric D. Shaw (2022). "The Critical Pathway to Insider Risk Model: Brief Overview and Future Directions." Counter-Insider Threat Research and Practice 1(1).

[13] Schoenherr, Jordan Richard, Kristoffer Lilja-Lolax, and David Gioe (2022). "Multiple Approach Paths to Insider Threat (MAP-IT): Intentional, Ambivalent and Unintentional Insider Threats." Counter-Insider Threat Research and Practice 1(1).

[14] Moore, Andrew P., Carrie Gardner, and Denise M. Rousseau (2022). "Reducing Insider Risk Through Positive Deterrence." Counter-Insider Threat Research and Practice 1(1).

[15] Zegart, Amy B. (2017). "The Fort Hood Terrorist Attack: An Organizational Postmortem of Army and FBI Deficiencies." In *Insider Threats*, ed. Matthew Bunn and Scott Sagan, pg. 42-73. Cornell University Press.