ARLIS IRiSS Event Summary

29 June 2021: Tools, methods, and technology: State of the art in modeling

This ARLIS event featured three guest speakers: Jeffrey Dodson, Katherine Hibbs Pherson, and Andrew Moore (speaker titles and bios appear on the IRiSS website event description). They responded to a series of moderator questions they received in advance along with and real-time questions posed by the event attendees. This summary is a high-level overview of responses to those questions. Following is a list of the question themes to help illuminate interests from the attending community. To help shorten the summary length and distinguish responses from the speakers and attendees, contributing conversation from the ZoomGov attendee chat is omitted.

Executive Summary

This session covered a wide range of topics for modeling Insider Risk. Much of the focus pertained to successful modeling, understanding what is good, obtaining and adapting new information into models, communication, and understanding boundaries and challenges. Lessons learned include that everyone working on Insider Risk should be a modeler, with some degree of conceptual to technical capability. Understanding boundaries on risk conditions and acceptable loss informs discussion of what will be acceptable risk, and this is best guided by leadership. We should broadly seek out new information for models across disciplines, sectors, and media formats; seek to bridge the three investigative tracks – HR, ethics, and security and be inclusive throughout the organization. We need to focus less on the individual, more on context; less on process, more on outcome; less on easy but less valuable models, more on thoughtful model design and sources of information.

Summary

Modeling Insider Risk is a journey which occurs within complex environments over time. It is tough to know when we achieved success and therefore harder to accomplish. Thus, obtaining nominal baselines are hard and we need to do better at tracking our efforts and effectiveness over time. Modeling is more successful when we incorporate other disciplines, increase our focus on impact and outcome, decrease focus on processes, and improve the agility and speed of our identification outcomes, while reducing the false alarm rates. We become more effective and efficient when everyone involved seems themselves as a modeler and part of the modeling venture, enhancing problem solving perspectives and cogent outcomes, which should also reduce company resource waste. All involved should understand both threat and impact but separate them in modeling. Useful measures include reducing organizational loss and better decision making. Existing quantitative frameworks can help, such as FAIR or Applied Information Economics, but we need to focus more on the context and less on the individual. Trusted Workforce 2.0 (TW 2.0) will hopefully bring some this needed rigor.

Good technologies help modeling efforts but must be useable by decision makers. Such tools and technologies should account for external factors and have commonly understood indicators. Technologies are even more valuable when they help us anticipate rather than predict and focus more on context. Without context, risk modeling can be self-reinforcing and

those that do not sufficiently consider organizational policies and practices can exacerbate risk. The modeling technologies landscape is large and evolving. Some techniques do well to model observable behaviors but less so when mapping to actual behaviors. Critical path models and diagnosticity are important approaches for identifying valuable models and factors, as well as help evaluate sources of information and actionable decision-making speed. Looking for what is different circumstances rather than normal (*e.g.*, a layoff) can help modify sensors before an event occurs. It is possible to use multiple tools in combination, but this requires thoughtful design.

Going deeper into computational modeling, we are moving away from intuition-based models. We can develop theory from modeling and document emergent aspects of threat to understand purpose behind it and reduce false positives. More traditional computational modeling such as Agent-Based Models (ABM) and system dynamics help to map emergent threats, whereas newer AI/ML approaches focus more on the risk scoring part (Bayesian) probability scores. Newer modeling leverages machine learning and behavioral analytics (such as UBA to UEBA or fraud detection) and there is a sense that we can continue to get better at collecting information and understanding the 'behaviors' they indicate. Yet, we should not lose sight that while modeling helps us look through bigger haystacks, and when we identify a needle, we still rely on human intuition for sense- and decision-making. Treat models as alerts that can be biased and think of them as another smart person on the team sharing their input.

Obtaining and adapting new information allows us to update our Insider Risk modeling efforts. Discussion forums, like this IRiSS, and interaction opportunities with academia or industry can offer modeling approach previews and stress testing. Internal employees can also be a wealth of information to learn more abut situations, procedures, and practices—be intentional, diverse, and collaborative with them to develop and gain feedback on indicators. Just about any source is a potential information reference, such as books and blogs, particularly those that discuss how individuals cope with change. Having an ongoing, varied, wide intake of new information can help anticipate change. Familiarity with PESTLE analysis and Cukier, Mayer-Schönberger, and de Véricourt's book "*Framers: Human Advantage in an Age of Technology and Turmoil*" were highly recommended.

Insider Risk modeling does not occur in a bubble. Modelers should communicate with HR and IT; these groups are key data owners and models benefit from their expertise. Anyone within the three investigative tracks (HR, ethics, security) should regularly also be at a common table to discuss behavior ambiguity. Average workers could strongly benefit from engaging with modelers. This has the added benefit of improving Insider Risk perceptions, advocacy, and overall better workplace support. Legal should be included as needed, particularly when models and subsequent decisions become increasingly complex with respect to privacy and rights. Modeling is not necessarily limited to the modelers. Everyone working on Insider Risk should view themselves as a modeler, possessing at least some modeling knowledge which can be based on something, such as the adjudicative guidelines, and interpreted through their individual personal perspective (framing). Models are getting sophisticated enough that we might be able to reverse-engineer decisions people made.

Limited resources can affect where modelers draw the proverbial line between what is or is not acceptable risk. Quantifying acceptable risk lines require quantifying acceptable loss. Leadership plays a key role to help set risk appetites, clarify risk condition boundaries, and discuss potential harm to the organization's reputation. Tabletop exercises can be useful to activities to explore these limits. Certain issues, such as extremism or workplace violence, may have their own thresholds; however, there may also be legal considerations as previously noted. Previous baselines are useful comparatives, and these records should be maintained over time.

Challenges can exist when attempting broad or intentional including of organizational factors and cultural information into Insider Risk modeling. Insider Threat was largely considered the domain of traditional security and compliance, but this does not fit reality well. Risk management is far more interdisciplinary and the 'not invented here' mentality does not work. Input from other operational and academic fields that help us understand society can help boost decision-making, particularly given the increased speed and volume of data which are shaping opinions and actions. This intentional inclusion also helps understand context, offsetting claims that organizational measures and social factors are hard to quantify. Until we deal with context in modeling, problems are bound to repeat when part of the problem is found in that context.

Moderator question themes

- Success in modeling for Insider Risk
- Modern tools and technologies
- Detection and misses
- Finding and adapting new information into modeling
- Communicating with modelers

Attendee question themes

- Where to draw the risk lines
- AI/ML vs. traditional computational modeling
- Role of culture and balance
- Challenges to intentional changes in Insider Risk modeling