ARLIS IRiSS Event Summary

17 August 2021: Actualizing the Insider Risk Paradigm

This ARLIS event featured four guest speakers: Tara Jones, Robert Rohrer, MJ Thomas, and LTG (ret.) Darsie Rogers (speaker titles and bios appear on the IRiSS website event description). This event is the capstone following five IRiSS events—each focused on a key area of discussion. Where previous events asked speakers targeted questions, this event asked speakers to provide reaction-style comments to key takeaways from the previous IRiSS events which were provided in advance; speakers also responded to real-time questions posed by the event attendees. This summary is a high-level overview of responses to those comments and 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

Overall, the speakers largely agreed with previous takeaways and expanded on them. Major focus areas include heavy reliance on leadership and recognizing the interdependent relationships between security, counterintelligence (CI), human resources (HR), and other departments with recommendations for increased collaboration. Organizational culture and the importance of trust and positive, empowering environments play an outsized but underused role in Counter Insider Risk (CInR) programs. Echoing throughout the entire session, CInR programs have a dual role as supporting and being supported by people. As such, speakers firmly rooted CInR as human security and identified individuals as the most important focus, juxtaposing to the modeling event takeaway. While these issues remain sociotechnical in complex, multidimensional systems, there was a recuring interest to reduce our reliance on technology—there are no technological silver bullets that produce ground truth. Other key interests included strengthening security and Insider Risk (InR) efforts by tying them to funding and baking security into contracts with clear consequences. Speakers admitted we have much still to do and acknowledged this event as a robust discussion focused on the right direction.

Summary

Part one – Panel reactions to previous IRiSS Event Takeaways

The five IRiSS events leading into this capstone session focused on the following topic areas: kickoff on changing the Insider Threat (InT) narrative to Insider Risk (InR), academic environments, industry views, modeling, and workforce supply chain challenges. This section features a summary of speaker comments linked to a takeaway from each of the previous events.

Kickoff event takeaway: *The kickoff takeaway noted that a shift from Insider Threat to Insider Risk must include a narrative change requiring empowerment, trust, and sociotechnical solutions without being singly reliant on people or technology.* Speaker responses fall largely into three focus areas: the narrative, security, and people and technology. Regarding narratives, all speakers agreed that words matter, but they varied opinions on the extent and impact of which InT and InR terminology mattered. To some extent program implementation may be more important than the terms we use to describe those programs. Yet, terminology can provide program scope, influence indicators and measures used, and shape perspectives about such programs. Incorporating multiple disciplines will also affect terms used and how we coordinate strategy. We can recognize the paradigm shift when we can address systems that fail individuals from individuals that fail systems. The paradigm shift also helps address issues of scale and leaders knowing their people. In addition to the social & technical convergence is a multidimensional security convergence of human, physical, and cyber domains. No program will be successful if it ignores the human domain. CInR is largely human security, and any paradigm shift should be rooted in the empowerment, trust, consideration for preemptive and proactive efforts to protect the people. Thus, this is a human problem more than it is tech problem. Tech has its uses, but it still requires people to make the tech useful from development and setup to operation and interpretation. Conversations should consider where we focus our attention, such as the new and growing number of vectors in which people, technologies, systems, and networks can be compromised, as well as how to keep ahead of vulnerabilities in positive ways before others exploit them in negative ways.

Academic environments event takeaway: *The academic environment takeaway noted that collaboration between the research community and security remains a great challenge and natural friction source; more and better risk/impact data can help bridge difference in priorities between these groups.* There will always be healthy tensions between security and academia regardless of CInT or CInR program efforts. Security in the academic environment is largely seen as a black box admin issue rather than security specific. Moreover, organizational culture differences make it hard to share data and address InR issues, even among security and CI professionals. These differences reinforce information insecurity and adversaries benefit from this gap, by reverse engineering stolen tech and research; like baking a cake, you can figure it out by knowing enough of the ingredients list. First step is to admit having a problem. Ongoing, directed, and open communication between groups can help unpack that black box and increase CInR within the environment. Senior leaders must direct, enforce, and assure data is shared in these communications. They can help incorporate lessons from the operations security (OpSec) and intelligence communities to integrate information sharing for better risk calculations. Some speakers favored tying federal funding to security requirements which can motivate InR program dialogue. Researchers may better understand the InR narrative if it is tied to their funding, compromised research, and ability to publish. DoD changes in funding requirements and communication efforts is already receiving buy-in from some academics.

Industry views event takeaway: *Some of the best actions are designed to be pre-emptive: sharing examples of good outcomes, strengthening leadership support and partnerships with government and across industries, expanding equity, diversity, and collaborative professional programs within the organization.* The speakers largely agreed that leadership is one of the core components for the success or failure of CInR efforts. Leaders must support those efforts and ensure everyone in the organization and other relevant stakeholders understand their respective InR roles, areas of overlap across departments, and the larger picture. Make this part of organizational culture. This workforce engagement can foster a sense of belonging, diversity, equity, inclusion, and trust—these elements are essential, not just soundbites. Be cognizant of people and groups that could alienated by CInR programs just as they could be targeted by external influences; do not create additional vulnerabilities. Likewise, be aware of people and groups that are intentionally in high stress situations, such as special operations, and the related inherent risk. While we cannot fully prevent affiliated risks, we can seek to recognize early signs, such as being overwhelmed or disgruntled, and allocated the necessary resources to help our people. For external stakeholders, if InR is not baked into a contract, people will not do it or invest money into it. Ensure contractors have their own CInR measures. Internally or externally, ensure we are not delivering or receiving compromised products, vet the entire supply chain. This may require additional education to better grasp the range of components used in your systems and processes and how they mesh with security and InR. Part of this effort must (re)prioritize security matters. Empowering leaders to do well also means they are widely educated and advised on security and InR issues since many leaders do not have these specialized backgrounds.

Modeling event takeaway: *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.* Of all the takeaways, speakers seemed to contrast with this takeaway the most. There was general agreement that context remains important to inform how we can better protect ourselves and our people. However, not focusing on the individual was described as counterintuitive as individuals are the key to managing InR and our best source of information. Whether process or outcome, the speakers framed the workforce and work environment as essential elements. Inclusive environments with proud, united, and empowered employees identify and mitigate InR, but can also be useful for modeling discussions. This may help offset challenges with building security models where the whole landscape changes as soon as you have a working model. Thoughtful models benefit from wider engagement to help identify the right amount and type of data needed; enough is needed for security analysis and to motivate people but not so much that people feel untrusted. More attention is needed for modeling at scale, where it is not as realistic to focus on individuals.

Workforce supply chain challenges event takeaway: *Insider Risk programs should span from hiring to separation; hiring and continuous vetting benefits from deliberative, proactive, collaborative engagement between HR, legal, security, employee relations, and other relative departments and stakeholders.* On this portion, the speakers agreed entirely with the takeaway, their comments discussing coins, collaboration, and culture. Human threat and human capital are different sides of the same coin. They are both concerned with motivation, ability, opportunity, just for different purposes. Both sides of the InR and HR coin must be involved through the entire employment lifecycle. We need to build trust into that lifecycle, which can be done through collaborating across departments and with other stakeholders that overlap with InR. Security professionals must understand these interdependent collaborations which can develop better whole-person perspectives. Broad engagement boosts local level and individual engagement, which are key aspects for trust building. These interactions benefit positive organizational culture change, although change can come slowly depending on the organization's current context. Org culture affects everything from recruiting, screening, and onboarding to understanding better ways to adjust resources and capabilities. It is also fundamental for asking how to help others and get others to ask for help.

Part two – Open Q&A discussion

Attendee questions coalesced into three categories: individual matters, things that affect the organization, and improving CInR efforts in general. The first thing to understand about individuals is that it is entirely possible to get 'left of boom.' However, we must see InR fundamentally as a human problem with a human solution and acknowledge our success depends on how well the programs are proactively engaged by the workforce. Technology will never give us the ground truth, so we build a better foundation with people.

Leaders as individuals maintain 100% responsibility for CInR, but they need metrics to help drive change. Help them by being open and seek audits, possibly from outside assessment, that give metrics to know what is strong and where we need to improve. Understanding the impact of not acting applies to both individuals and organizations.

More stick than carrot may be needed to motivate entire organizations and the people within. Carrots involve adjusting incentives and funding requirements to improve security and accountability. Sticks make this clear in contracts and incorporate steep consequences, such as financial or reputational costs, for violating security principles. Design contracts to match threats and risks but understand contracts may become outdated. These efforts should echo through all of your supply chains, acquisition security, and related policies. Collaboration between departments improves ongoing communications and outcomes while breaking down silos. HR, security, and CI, share a symbiotic relationship. Stronger organizational relationships fill information gaps and whole-person concepts.

This series seeks to move the paradigm shift dial from CInT to CinR. Both build on the same model of motivation, opportunity, and ability. Likewise, both can promote and empower the good to prevent the bad. This shift is in-part a cultural one that requires building trust with employees, empowering leaders, and educating stakeholders to focus on a risk environment in which we mitigate the behaviors before they manifest. Some of this should consider American cultural aspects of an individualistic society rather than one that favors the greater environment. Narrative and perceptual changes benefit from increased human intelligence and a reduced reliance on technology. Resources to widely boost CInR efforts are available through the CDSE's trainings and their Sentry app, as well as online information from DCSA, DITMAC, and PERSEREC.

Moderator event takeaway themes

- Narrative shifting
- Natural friction between security and research community
- Pre-emptive actions, leadership, and partnerships
- CinT/R modeling scope changes
- Workforce lifecycle and organizational engagement

Attendee question themes

- Early employee risk prevention
- Offsetting contractor lack of interest
- InR expenditure justifications
- InT and InR as separate missions
- Recommended InR resources
- How to engage management
- Magic wand – any one change