ARLIS IRiSS Event Summary

25 May 2021: Industry Views

This ARLIS event featured three guest speakers: Stephen Szypulski, Caroline Gilman, and Dr. David Mussington (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 event focused on industry views with panelists providing insights from their own organizations as well as experience gained through collaborations. The session was highly interactive and even when the speakers did not agree on a given topic, areas of overlap were apparent suggesting common approaches. Lessons learned included that industry is generally good at understanding risk widely, so thinking about Insider Risk as part of the larger risk ecosystem allows use of a wider range of management tools, practices, and perspectives. Changes from threat to risk occur through intentional and actionable inflection points that work best as ongoing, supportive, and inclusive initiatives at the organization's grassroots level. Also, 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.

Summary

To help with a baseline for our discussion, it is important to understand how our panel distinguishes between Insider Threat and Insider Risk. Insider Threat was seen as micro level, destructive, and event based, personified in individual, intentional behaviors. Insider Risk was shared as a macro level paradigm and as a highway intersection analogy using a traffic light as an indicator of risk within the intersection. Risk was also defined as a function of vulnerability and threat. Risk can be managed, mitigated, but also multi-causal and therefore more but it is difficult manage. Moreover, risk and threat have different conceptual and contextual meaning within organizational culture. From a cybersecurity perspective, the term 'insider' is problematic. Who is considered an 'insider'? If you are a cyber organization, being an insider is part of your most important identity; then the notion of an insider / outsider is a barrier to the most effective risk management. Notably, Booz Allen Hamilton (BAH) intentionally started their program with an Insider Risk grounding rather than Insider Threat.

Our panelists took slightly different positions when we extended the concept of Insider Risk as part of a larger ecosystem. One speaker viewed potential failure modes as a crowded field when looking across a whole company; Insider Threat is just a part of it, addressed by prevention programs. Another speaker didn't see Insider Threat as a failure mode; instead, their company expects employees to maintain long standing business principles of honesty and

integrity—or viewed differently, principles could be seen as managing types of capital: intellectual property, people, financial. The third speaker situated Insider Threat as part of an evolving six-step activity / action process. Each stage is part of the ecosystem where teams can seek to mitigate Insider Risk.

Flipping the conversation to building trust and resilience (T&R) as work, each speaker offered a mix of insights from their respective companies, but all views centered on the importance of supporting employees. T&R are transient and changeable, improved by clear, transparent, and actionable steps within the organization. T&R starts at grassroots level between employee and supervisor. Build foundations of trust with accountability and promote the business culture. This includes fostering a culture of inclusion, diversity, and addressing equity issues. T&R-building support can happen at inflection points, such as onboarding and promotions. Managers should know and show up for their people, supporting different perspectives and reducing group think. This can be echoed at the team level. At an organizational level, it can develop through tangible and intangible benefits such as wellness programs. All such efforts can have metrics, allowing for accountability reviews. Thus, organizational resilience can be a measurable target. As organizations change, reflect on where and how T&R can be strengthened, let employees know they are supported. BAH moved away from annual assessment to a monthly conversation of constructive feedback and to build rapport; this helped with the move to remote work. Daily successes can lead to long term success but won't without intentional actions to make it happen.

Every good industry panel offers some best practices and other advice. Best practices for government included: be more sophisticated about operational risk, use metrics and sophistication of risk management tools; include diversity and be intentional about how you go about challenging/changing the status quo of programs; and foster collaboration, the better they collaborated in their industry hub, the better they did. In addition, create professional pathways within the organization to target Insider Threat and equity, diversity, culture, organizational factors simultaneously with metrics and accountability reviews to ensure those pathway programs are successful. Find opportunities, such as this IRiSS event, to share good, specific program examples, which may help offset potential bad industry or 'Big Brother' reputations. Think beyond budgetary limitations to discover benefits in low/no cost things such as leadership support and partnerships. Try to be forward thinking to be proactive instead of reactive—leverage partnership and do not ignore signals or wait for a technological silver bullet. Develop policies and procedures that provide courses of action when specific event clusters occur, like a guidebook which gives more predictability and reduces managerial burden. Acknowledge your Insider Risk program gaps—many programs are relatively new and it can be hard to show metrics/results, others grapple with the problem of limited resources and where to you focus efforts.

Attendees were curious about the types of products and tools used to address Insider Risk. CISA uses granular, climate-style surveys with follow ups that focus on attitudes towards mission, attitudes towards leadership, and fairness within organization. CISA treats culture and Insider Risk management as a business line where you have improvement plans. BAH uses a

suite of critical tools: monitoring, forensics, case management systems, but they are not end as the tools change quickly, evolving with feedback. Meanwhile, it remains important to pare down to the informative metrics. Goldman Sachs uses big data analytics and include metrics such as incidents and training, but steer away from metrics on firings. They show success to leadership through value saved in reputational impact and loss of intellectual property, items that do not offer the same traditional measures as other business lines.

Culture and was a recuring Insider Risk theme raised by the panelists. Culture-related metrics can be found by working closely with human resources (HR). Seek data from employee assistance programs (EAP), retention of employees, and violations of ethics or conduct codes. Where available, use custom surveys, such as FEDS (an annual federal employee survey), to track trust in leadership, trust in interventions, if organizations live up to their values, and if organizations match up to their public declarations to address employee issues/grievances. Despite established organizational cultures, some insiders may maintain their own agendas. Such agendas may arise based on combination of motivating factors, such as financial, psychological, or situational. Part of the Insider Risk job is to learn of those motivations, cultures, and other contributing factors. Juxtapose these factors with resource management challenges—allocate based on insider and other types of threats.

Another area of attendee interest were bystander challenges, which occur where people often sense something's not right with a colleague but usually fail to bring that to an organization's notice. Such events are common in industry, but continuous training helps. Include what is considered ‘normal’ and provide clear lines of communication for employees to use for reporting. Ensure the training includes empathy for diversity and inclusion issues; empathy in an organization can go a long way. While it is possible that employees volunteer or could be recruited to behave outside the norm, none of the speakers found this to happen in their organizations even with their Insider Threat and employee motivation analyses.

<u>Moderator question themes</u>

- Distinguishing between Insider Threat and Insider Risk
- Insider Risk within a larger ecosystem
- Building trust / resilience
- Best practices and advice

<u>Attendee question themes</u>

- Bystander challenges
- Individual agendas
- Insider Risk product/tool use in teams
- Metrics for measuring culture
- Gaps in Insider Risk programs