The views expressed in this article are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

ARLIS IRiSS Event Summary

26 April 2021: Gain & loss, response, and management around insiders within academic environments

This ARLIS event featured two guest speakers: Dr. Laurie Locascio and Dr. Kevin Gamache (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 issues of Insider Risk within the academic environment. The session had a highly engaged audience and the speakers largely agreed with each other, building upon each other's detailed responses. Lessons learned include 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. External relationships with government partners are critical, mutually beneficial, and evolving as we learn from each other; and unlike government and industry relations, copy & paste best practices does not work. Also, when Insider Risk programs are working well, it will be like a good cybersecurity program: invisibly running in the background, but massive failures can result in lasting damages to an ability to innovate at individual academic, university, and national levels

Summary

The event started with a baseline to understand our speakers' thoughts on Insider Risk and how it differs from Insider Threat. Both speakers use a widely accepted definition of Insider Threat as the foundation (ref. CMU SEI link), Insider Threat centers on the individual as a threat source of organizational damage and the solution is to eliminate the threat, which does not work well for the individual or organization. One speaker's metaphor provided the internet as a threat which is eliminated by unplugging the computer, but then you don't have internet. Conversely, they saw Insider Risk as a more balanced approach looking at risk and benefit with an understanding that there will always be risk and so we use controls to manage it. Insider Risk is more data centric, refocusing from centering solely on the individual to a more holistic approach of understanding data risk. Neither speaker had a better term for where we should be than Insider Risk; however, suggested that we should maintain risk awareness rather than risk aversion, particularly within an academic community. Moreover, Insider Threat terminology and programs that focus on the individual, as reflected in some mandates with DoD or DoE, set choices that make the academic community ineffective and are dangerous to a university.

Insider Risk requirements can help prevent integrity loss of research, facilities, and people. There isn't much that is black and white in Insider Risk; every risk we evaluate comes wrapped in a shade of grey. Each of us represents some level of Insider Risk and there are many ways to find warning signs. There are no absolutes and sometimes knowing the direct consequences of actions is preventing something. For example, an agreement externally vetted was turned down because a subsidiary was associated with human rights violation and turns out later that the company had a known history of tech theft. University research offices also help investigate integrity issues of bringing non-contracted data between institutions.

Yet, Insider Risk results vary and successes resulting in pyrrhic victories, where the costs to the research were excessive, remain a regular challenge. Pyrrhic victories are huge in the academic community. They are a challenge unique to the academic research enterprise given a foundational principle is sharing information. Every security policy must account for this organizational and operational design. Every agreement we pass on can alienate the country or collaborator or can devastate an academic career. Success is protecting the person, university, country, but we never know in the moment all the consequences and the size of the victory. Focusing on the individual is problematic as most Insider Threat ‘indicators’ from industry and government are the expected behaviors of academics. Another focuses heavily on foreign born individuals and the potential for foreign influence, and yet 30% of US Nobel prizes are won by foreign born but US educated researchers. Ultimate pyrrhic victory is the problem of higher education – do not stifle the research enterprise.

Integrity loss is often discussed in terms of Insider Risk from foreign influence, but it can happen from US domestic sources as well. It is a balancing act to train individuals who may become future competitors, but there is an expectation for those individuals to innovate rather than clone the research. Although researchers tend to be good at protecting their info information to avoid being scooped. Yet, intellectual property is still stolen, regardless of whether it goes to Idaho or Italy. So, it remains important that Insider Risk management processes, like collaboration and Conflicts of Interest, are organizationally agnostic. If a foreign government operates through a domestic organization, it would be hard to know and it helps to coordinate with other academic institutions.

Onboarding the research community regarding Insider Risk awareness and have people accept it as a real risk remains a salient challenge. One speaker went further, claiming there is no greater challenge than securing research enterprise without interfering with collaborate culture and innovative enterprise. Security policies largely operate in the background, such as vetting collaborators. Sometimes this requires risk mitigation decisions the research community does not like. This is complicated sometimes by a lack of understanding or acceptance that the threat may outweigh benefits of open research, collaboration, and the free exchange of ideas. Communication here is key, supported by data to justify Insider Risk decisions and discussed in ways to account for academics’ different priorities, such as loss of grants rather than intellectual property, how to communicate without being isolationist, and value our international collaborators and science community.

Relationships with US government security agencies, such as the FBI and DCSA, are critical to Insider Risk success within academic environments. Substantial, mutually beneficial partnership efforts on both sides cultivated a sense of trust and truly collaborative culture. These efforts are long-standing over many years and joined by universities across the country. Despite mutual interests between academia and national security, natural friction remains due to different their missions. Both sides continue finding avenues for complimentary fit and coordination. Active engagement helps government understand how academic culture differs from industry—copy/pasting practices and polices across sectors does not work. Developing Insider Risk programs individually is very costly, and academia benefited greatly from its security agency partnerships with enhancements in areas such as personnel vetting and risk assessment; yet there is still room for improvement, particularly with getting ahead in global competition.

The US government requires disclosure about funding from foreign influences and a 2020 Department of Education report from detailed substantial shortcomings in reported funds. One speaker's university was one of those asked to become compliant, but the non-compliance was not nefarious; rather, university administrators found the way the rule was written made it hard to report. They are now compliant and focusing more on compiling federal laws. Transparency is fundamental for risk awareness. The issue is not about a faculty member having a foreign talent contract, but rather the lack of transparency regarding that contract.

Balancing between Insider Risk needs and faculty interests for free and open expression might give the impression of Big Brother. This impression is avoidable by having every PI involved in the Insider Risk process. Training is highly effective, improving their risk knowledge and detailing consequences helps mitigate risk. Bring the academic community together on Insider Risk and being vigilant. Included in training should be clear IT policies and expectations, particularly regarding any monitoring. The balance line is also seen as an amount of risk tolerance, which differs by institution and cannot be a blanket policy. The funder, nature of research and personnel involved, reputational risk, risk to students, and loss potential and impact can all affect tolerance, creating a mosaic of cases. Regardless of risk tolerance, it is helpful to proactively reach out to reach out to researchers who are in areas that are high risk or have relationships that are high risk for additional training one on one training. Provide allowance for Q&A; faculty tend to become ambassadors to other faculty. The process is quite intensive but prevents the 'checkbox' mentality and improve coordination.

A final Insider Risk scenario in the year 2035 allowed the speakers to illustrate how things could go very differently. One speaker addressed an ideal outcome where a strong Insider Risk ecosystem felt invisible. Awareness, updates, and training kept everyone current and without feelings of paranoia or distrustful; it is an open and collaborative time where everyone plays their part. The other speaker painted a grim vision where the US academic research enterprise is no longer the best in the world and the US economy is no longer the strongest. The linchpin was universities' failure to address foreign influence challenges with significant cascading loss effects of research data and expertise. Also contributing, Congress legislated solutions that didn't fit the unique academic environment, which stifled the free flow of information and ideas that were the hallmark of universities for centuries. We lost an ability to innovate.

Moderator question themes

- Differentiating Insider Threat and Risk
- Preventing loss & pyrrhic victories
- Challenges with onboarding the research community
- Domestic, not foreign, organizations
- Relationships between academia and US federal security agencies
- It’s 2035, what happened.

Attendee question themes

- Funding and foreign influence
- Security without being Big Brother
- Insider Threat, poorly named concept
- Risk tolerance
- Moving data between institutions
- Lack of trust
- Checkbox training and attitude and behavior change