Talking to Academics about Security

Student Guide

August 2021

Center for Development of Security Excellence

Introduction

Welcome to the Talking to Academics about Security Short.

The purpose of this course is to inform Research Security, Facility Security Officers, or FSOs, Counterintelligence Special Agents, or CISAs, and other security personnel who work with scientists, engineers, and others within cleared academia about the unique challenges that present themselves when talking to academics about security. Scientific research has its own culture with unique motivations. Talking with this audience requires different lines of persuasion when talking to them about security. In this course, we'll discuss why this is and make some suggestions for how to connect with an academic audience.

By the end of this short, you will be able to communicate security fundamentals effectively to cleared academia, scientists, and engineers who rely on foreign collaboration.

It should take about 20 minutes to complete.

Differences between Academic/Scientific Communities and Security Community

This is Diane Aziz. Diane is a research engineer at a state engineering school.

As part of her research, she's working on advancing new airfoil technology with improved stealth capabilities.

Like many of her colleagues, Diane is accustomed to working in an extremely collaborative environment. By working together with others, she and her team are able to develop extremely innovative solutions and discoveries. Collaboration is a key part of her work, and this is often the case with scientists and academics from around the globe.

Diane is extremely respected in her field. She's known throughout the industry as a leader in stealth technology. She's proud of her accomplishments. Her two biggest motivators are the advancement of science and the accolades she receives.

In her latest research, Diane works closely with airfoil engineers from Germany, also some of the top researchers in their field. This cooperation is crucial to her latest project. She's apprehensive about how increased security requirements could affect her ability to get the information and innovation she needs. After all, the work she does will ultimately benefit U.S. security by making aircraft more difficult to track. Don't the benefits outweigh the risks?

Diane is not alone in her concerns. Many academic researchers worry about what security measures could mean for how they work. They fear that these measures may slow down the research progress. But ignoring security requirements could put them at risk, personally and professionally. So how can security professionals discuss security requirements in a way that puts researchers at ease while emphasizing the importance of protecting sensitive information?

History of DOD and Research Community Relations

The first step in tackling this issue is understanding the history of the relationship between DOD and the research community.

In 1982, a report by DOD and the National Science Foundation, or NSF, identified that university research and technology could be broadly divided into three categories:

1. Total Openness or Fundamental Research, where the benefits of shared information completely outweighed the risk, and thus could be shared freely;
2. Classification Necessary, where the research "demonstrably will lead to military products in a short time"; and
3. Dual-use between military and civilian, which is more of a gray area. In this category, more limited restrictions would be appropriate, but still advisable.

In 1985, National Security Decision Directive, or NSDD-189, included the recommendations of this report. This directive created policy that determined the flow of science, technology, and engineering information that was produced in federally funded research. At the time, the directive required that information be kept unrestricted "to the maximum extent possible." However, the understanding of these requirements has shifted in recent years. It also defined fundamental research as: basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.

See the resource page for more information on policy related to protecting research.

What Has Changed?

So, what caused the change? Well, in recent decades, there has been an increase in foreign exploitation of intellectual property, or IP. Some governments are thwarting or ignoring the safeguards designed to protect IP. Also, the U.S. has seen an increase in foreign economic and military competition rather than cooperation.

At the same time, there has actually been an *increase* in scientific collaboration between the U.S. and researchers in other countries. Data shows that there is a heavier reliance on bilateral cooperation between China and the U.S. than any other single country. We have seen that our allies also have deep research ties with China and other competitive governments.

We have also seen an increase in the dual-use category of research. The technology that proves advantageous to our daily lives also has more and more significant strategic value in military and intelligence applications.

The demographic of researchers in the U.S. has also changed. One third of U.S. PhD recipients are temporary visa holders. These are foreign citizens who have increased vulnerability to targeting by threat actors.

And there have been examples of high-profile information security lapses through compromise of academic research. The 2nd Obama administration tightened security at U.S. National Laboratories due to the leakage of sensitive technologies.

Lines of Persuasion

So given this situation, how can you talk to the academic community about the risks in a way that will be most impactful and help them understand the importance of security? There are certain lines of persuasion that tend to resonate best with this audience.

The broad categories are:

- Personal and Professional Risks
- Consequences of a Security Breach, and
- Protecting National Security

Personal and Professional Risks

The first category of lines of persuasion are those personal and professional risks to the individual. Remember Diane? Two of her major drivers are her professional reputation and pride in her accomplishments.

If Diane inadvertently divulged sensitive information to someone with ill intent, she could lose the credit for her authorship and the recognition for her work. With someone else taking credit for her research, her reputation and prestige would be at stake.

In addition, with someone else at the helm, she would lose control over her research; the data she wants to present; the way it is presented, shared, and used; and any technology that might result from that research.

Diane might ultimately lose her job and her income because of the lost data and disclosure of sensitive information. Not only that, but the damage to her reputation could put her future employment and research opportunities at risk as well.

Consequences of a Security Breach

If the government determines Diane caused a security breach, it will likely take legal action against her, which could result in fines or even jail time.

This action could result in her losing her personnel clearance, or PCL.

The impact of a breach could extend to Diane’s co-workers and their families and businesses as facilities close and research halts.

In addition, these charges can create a stigma tarnishing her or her company or institution’s reputation, which could jeopardize future employment opportunities and contract awards.

Protecting National Security

Diane, like most academic researchers, is focused on advancing science and technology.

U.S. citizens can be presumed to be loyal unless evidence to the contrary is found. Most foreign nationals conducting research in U.S. labs are intent on their work and keeping the oaths they took to protect confidential information.

But scientific research is also about collaboration. In this setting, appealing to a sense of civic duty or patriotism may not be as effective as other lines of persuasion. It's important for the academic community to understand the consequences of a security breach.

Diane has a nephew that is currently serving in the Air Force. If there is a security breach and the enemy gains access to Diane's stealth technology, this could potentially increase the danger to her family and friends.

For researchers that are not working directly on equipment with military applications, there is still the risk to economic stability as foreign adversaries are able to bring technology to market quicker and cheaper without having to budget as many resources for research.

In some cases, a security breach could transfer sensitive technology to other unforeseen nations. Some countries may engage in "technology brokerage," selling our technology to other countries. So a "friendly" nation may obtain our technology and sell to "unfriendly" nations. And a security breach might also result in the transfer of technology to regimes that will use it against the U.S., either its military or the home front.

Common Attack Vectors

Diane has spoken with her Facility Security Officer, or FSO, who emphasized the impacts of information security to her personally and professionally. She understands the importance of protecting information and wants to know what to do.

If the research is a classified program, Diane should check the Security Classification Guide, or SCG, for information about classification levels. She should also review the Program Protection Plan, or PPP, for her facility. For proprietary data, there should be company or institutional guidelines available. The FSO should explain some of the common vectors adversaries use to acquire sensitive research information.

Research fellowships involving foreign nations are possible vectors of attack. It's important to note that research fellowship is a common practice in academic research and should not be avoided. But when taking part in these fellowships, Diane should know what information is sensitive and be particularly aware of who she shares it with.

Another common vector is research incentive programs. These programs provide financial and other resources to perform research in or for a foreign nation. China's "Thousand Talents" program has been a high-profile example of this. "Thousand Talents" recruits researchers from around the globe to set up labs in China. Again, these are common practices in academic research, and the U.S. has similar programs to recruit exceptional scientists. While these programs are not problems in and of themselves, Diane needs to be

aware of the rules regarding these programs, including how she receives and reports compensation.

Reducing Vulnerability

Diane's FSO tells her there are a few ways she can reduce her vulnerability to exposing sensitive information:

- Fully disclosing substantial contributions from other organizations, including foreign governments;
- Disclosing any financial conflicts of interest;
- Not divulging proprietary, classified, or otherwise sensitive information;
- Not sending information gleaned by participating in the peer-review process to other countries.

Connecting with Researchers and Academics

As a security professional that works with researchers and academics, like Diane, you should keep a few key things in mind when trying to convey the importance of protecting sensitive information.

First, remember that researchers and academics are key to advancing our understanding of the world and technology. Researchers and academics must balance the risks of divulging sensitive information with the need for collaboration. Be sensitive to this challenge and do your best to work with them to accomplish their goals while also mitigating any vulnerabilities.

One way you can connect with—and be heard by—researchers is to understand what they are working on. Take time before meeting to learn about their research topic and be able to speak about it with some basic familiarity.

As part of your discussion, understand who their partners are, how they are vetted, and the due diligence factors involved in determining vulnerability. While most research partners are not malicious, researchers need to be honest with themselves and with the security professionals about the potential vulnerabilities.

Building an understanding between your security team and the scientists, engineers, and researchers will foster a better understanding of the work. This in turn will assist in developing security countermeasures, and drive reporting of suspicious activities.

And finally, have concrete, data-based evidence of the risk specific to their work. This includes recent news stories about the consequences to researchers who allowed sensitive information to be disclosed or failing to disclose funding received from foreign nations. Or it could include statistics on economic damage from unprotected information, or the cost in human life or health. While patriotic and civic duty does have an impact on this audience, nothing speaks in volume like data-driven evidence.

Check on Learning

Which of the following lines of persuasion is least likely to resonate with a research and academic audience?

- ○ A. Risk of legal repercussions
- ○ B. Examples from the news
- ○ C. Loss of credit or authorship
- ⊙ D. Contact with foreign citizens is too risky

***Feedback**: Telling academics, researchers, and engineers that they should not have contact with foreign citizens is not likely to be effective, nor is it very realistic. This audience relies on collaboration with researchers around the world to perform their work. The lines of persuasion that are most likely to be effective are data-driven evidence and appeals to their reputation and career. If leveraging appeals to U.S. security interests, you should connect it to the impacts to them personally, such as effects on family and friends serving in the military.*

Summary

Thanks to a spirit of partnership on the part of her FSO, Diane has a better appreciation for the risks involved with sensitive information. She understands that by protecting sensitive information, she is also protecting herself, her family, and her co-workers.

In addition, she feels like her FSO is there to help her and her research rather than hinder it. The lines of persuasion focusing on the risks to her personally and professionally, the consequences of a security breach, and protecting national security resonated with her, and she's ready to work together to protect sensitive information while collaborating with her peers in a way that advances her research.