FBI

COUNTERINTELLIGENCE STRATEGIC PARTNERSHIP INTELLIGENCE NOTE (SPIN)

SPIN-15-006 JUNE 2015

Preventing Loss of Academic Research

INTRODUCTION

US Colleges and Universities are known for innovation, collaboration, and knowledge-sharing. These qualities help form the bedrock of US economic success. These same qualities also make US universities prime targets for theft of patents, trade secrets, Intellectual Property (IP), research, and sensitive information. Theft of patents, designs and proprietary information have resulted in the bankruptcy of US businesses and loss of research funding to US universities in the past. When a foreign company uses stolen data to create products, at a reduced cost, then compete against American products, this can have direct harmful consequences for US universities that might receive revenue through patents and technology transfer.

Foreign adversaries and economic competitors can take advantage of the openness and collaborative atmosphere that exists at most learning institutions in order to gain an economic and/or technical edge through espionage. Espionage tradecraft is the methodology of gathering or acquiring such information.

Most foreign students, professors, researchers, and dual-nationality citizens studying or working in the United States are in the US for legitimate reasons. Very few of them are actively working at the behest of another government or competing organization. However, some foreign governments pressure legitimate students and expatriates to report valuable information to intelligence officials, often using the promise of favors or threats to family members back home.

The goal of this SPIN is to provide an overview of the threats economic espionage poses to the academic and business communities. The Strategic Partnership Unit (CD-4F) welcomes your feedback.

WHO USES IT? HOW IS IT USED?

Foreign governments, foreign businesses, and competitors have sought to improperly or illegally obtain information from US institutions of higher education.

Foreign companies may provide resources, information, and competitive intelligence, on behalf of their indigenous government as a way to promote the overall economic well-being of their country, and to bridge research and development knowledge gaps with stolen information.

Foreign businesses may steal trade secrets, IP, proprietary research, and sensitive information in order to gain an economic edge or dominance.

While information is shared on campuses, there is still an ethical, and sometimes legal, responsibility to protect research. With the extensive amount of primary research done at universities, many academics hope to gain recognition for innovative research. When IP is stolen from academic institutions, they face not only the loss of potentially valuable information and technology, but also risk rendering obsolete the years of work and research that went into the foundation of the IP. Such a loss could preclude the ability to conduct related research and development in the future. Research is often funded by private companies or the government who may need a first-to-market practical application from the research to make it worth their investment. Stealing the research could then equate to stealing money from the funding organization/agency.

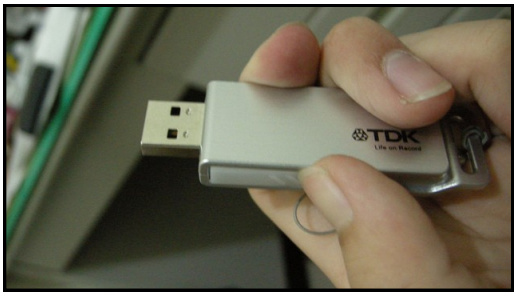
ACADEMIC ESPIONAGE TRADECRAFT

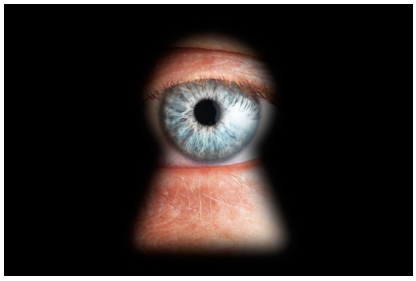
The following have been proven as successful platforms for academic espionage in the past and flourish in collaborative, open environments:

- Social media manipulation; using false identities to solicit sensitive information via the Internet.
- Academic event solicitation; using a conference as an opportunity to solicit sensitive information in person.
- Tour groups/delegation visits; pretending to be lost and wandering into sensitive areas, or to gain physical access to automated systems.
- Studying abroad; coercion and recruitment by foreign government agents masquerading as friends or patrons.

The following behavioral indicators warrant further inquiry to determine whether an individual is stealing research:

- Without need or authorization, removes proprietary or physical material out of the facility.
- Seeks or obtains proprietary or sensitive information on subjects not related to their research/studies.
- Unnecessarily copies material, especially if it is proprietary or classified.
- Remotely accesses the computer network while on vacation, sick leave, or at other odd times.
- Conducts research/studies at odd hours without a need or authorization (i.e. weekends, holidays, or relatively unusual schedules).
- Disregards organizational computer policies on installing personal software or hardware, accessing restricted websites, conducting unauthorized searches, or downloading confidential information.
- Short trips to foreign countries for unexplained or strange reasons.
- Unexplained affluence; buys things that he/she cannot afford on his/her household income.





- Engages in suspicious personal contacts, such as with competitors, personal business partners, or other unauthorized individuals.
- Overwhelmed by life crises or career disappointments.
- Shows unusual interest in the personal lives of co-workers; asks inappropriate questions regarding finances or relationships.
- Concern that he/she is being investigated; leaves traps to detect searches of his/her work area or home; searches for listening devices or cameras.

Many people exhibit some or all of the above to varying degrees; each suspected threat should be evaluated if some or all indicators are apparent.

Individuals and organizations that want to obtain valuable and restricted information may misrepresent themselves and their intentions in order to gain access to restricted information. Colleges and universities should identify their intellectual property, be cognizant of individuals and organizations looking to steal such information, and enact controls to mitigate such threats.

COLLECTION TECHNIQUES

Collection techniques vary depending on the type of technology being targeted. Techniques have changed and adapted as technology has advanced and will continue to evolve. Understanding espionage tradecraft can reduce the effects of being targeted. The following methods are used to target technology:

- Unsolicited e-mail.
- Front companies.
- Liaison with universities that have ties to US defense Contractors.
- Exploitation of research and facilities located overseas.
- Hacking.
- Circumventing export control laws.
- Visiting scientific delegations.
- Physical removal of data.

SOCIAL MEDIA MANIPULATION

In 2010, a US security consultant created fictitious accounts on Facebook and LinkedIn for a supposed cyber security professional, using photographs of a young woman found on the Internet and fabricated skills and work experience. The fictitious cyber expert, "Robin Sage", was able to collect almost 300 social network connections in less than a month's time, and included the sitting Chairman of the Joint Chiefs of Staff, the Chief of Staff for a US Congressman, and several senior leaders in the military and defense contracting arena. During the interaction, several instances of poor security practices, unintended personal disclosures, and military operational security violations occurred.

"Ms. Sage" was invited to speak at a private sector security conference, review a technical paper written by a NASA researcher, invited to dinner, and to apply for jobs. All of this occurred despite several obvious "red flags" that should have been apparent to anyone who took the time to read through her supposed job history and experience.

Several people did spot inconsistencies and tried to warn people away, however many people still chose to connect with Ms. Sage.

Anyone with an Internet connection can create such an account and gather volumes of personal, and potentially valuable, national security information in a very short amount of time.

ACADEMIC EVENT SOLICITATION

Academic events such as conferences, provide opportunities for collectors to surreptitiously collect valuable information and establish personal relationships for future elicitation and exploitation.

During a 2013 Unmanned Aerial Vehicle (UAV) conference in Washington DC, a three-page document was found on the convention floor. The document was in a Middle-Eastern language. Translated, the title referred to "Information Collection during the Conference and Exhibition."

Contextual clues within the document provided strong evidence it was prepared by or for a particular Middle-East company. The document tasked three nationals of the same country as the company to collect specific information on prioritized U.S. companies and technologies at the conference. One of the individuals so tasked was previously unknown to law enforcement, and had not appeared in previous reporting. However, the document contained contextual clues that he was an employee of the company.

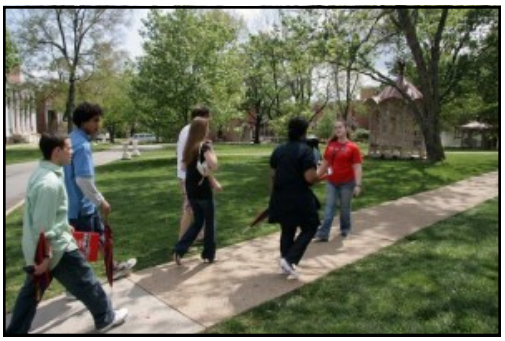
The discovered document instructed collectors regarding:

- What companies to target.
- What information to collect and report.
- Attending relevant events.
- Taking photographs.
- Obtaining copies of presentations.
- Clarifying terms.
- Collecting product lists, brochures, and advertising materials.
- Seeking client information.

TOUR GROUPS/DELEGATION VISITS

Visitors entering your work or research facilities could pose a security risk to your intellectual property or valuable research. Even seemingly innocuous information, such as the facility layout could be valuable in providing clues about your products, research, or processes.

Indicators that a visitor may be attempting to obtain restricted information include:



- Requests for information that is classified, dual-use (civilian and military applications), or otherwise controlled.
- Attempts to access or plug a device into a computer or system.
- Making last-minute additions or changes to the visitor roster.
- Bringing, or attempting to bring unauthorized recording devices into sensitive areas.
- Positioning/fiddling with a watch, pen, or a disguised recording device.
- Asks questions outside the scope of the approved visit.
- Acts offended/belligerent when confronted about a security or protocol incident.
- Wandering away from the group/pretending to get lost during the tour.
- Asking questions about programs/research of a sensitive nature that they should not necessarily know about.
- Attempts to keep security identification badge/claims "losing" badge during tour.
- Surreptitiously removing physical samples, such as using double-sided tape on the soles to pick up metal shavings, or dipping ties into chemical solutions for later processing and analysis.
- Unauthorized photography.
- Expressing unusual interest in/questioning of individual employees.

STUDYING ABROAD

US students and researchers are potential targets of interest for foreign intelligence services. Foreign intelligence services often develop initial relationships with US students overseas under seemingly innocuous pretexts such as job or internship opportunities, paid paper-writing engagements, language exchanges, and cultural immersion programs. As these relationships develop, foreign intelligence services may ask the students to perform tasks and provide information (which is not necessarily sensitive or classified) in exchange for payment or other rewards, slowly increasing their demands over time.

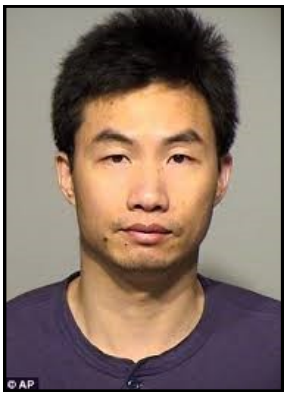
US students studying abroad have become involved in espionage activities in the past, and have been prosecuted for these activities. For example, American Glenn Duffie Shriver spent over a year of his undergraduate studies living in Shanghai as part of a study abroad program. After graduation from college in 2004, Shriver moved back to Shanghai to look for employment. Shriver answered an English-language ad soliciting someone with a background in Asian Studies to write a paper on US/China relations concerning Taiwan and North Korea. Shriver met with a woman named "Amanda" who paid him $120 for his essay. Under the guise of friendship, Amanda introduced Shriver to two men who Shriver came to believe were Chinese intelligence officers.

Amanda and the two Chinese men worked for the Chinese Ministry of State Security (MSS) and encouraged Shriver to apply for US State Department or CIA employment. While Shriver studied for, applied, and tested for such employment, the MSS officers paid him a total of $70,000. The goal of the MSS officers was to have a mole embedded at the US State Department or CIA. At the suggestion of the MSS officers, Shriver applied for a position with the CIA Clandestine Service. Shriver was eventually selected to apply in December 2009. At some point during Shriver's application process for the CIA, his activities were discovered and he was arrested while attempting to board a flight to South Korea in June 2010. In October 2010, Shriver plead guilty to conspiring to pass defense secrets to China's intelligence service and he was sentenced to 4 years in prison.

Prior to his involvement with MSS, Shriver had no criminal history and by his own admission was acting out of greed and the lure of "easy money."

RECENT CASE STUDIES

MEDICAL CENTER OF WISCONSIN



In February 2013, Hua Zhao, a research assistant at the Medical College of Wisconsin (MCOW), allegedly stole three vials of C-25, a patented compound used in Anderson's cancer research. During an internal investigation conducted by MCOW, security footage revealed Zhao entering Anderson's office and leaving shortly after.

Zhao was reprimanded previously for placing laboratory data on his personal computer. He was ordered to remove the data from his computer and place it on an MCOW computer. Additionally MCOW discovered posting by Zhao on an internet site, called Researchgate, indicating that Zhao discovered a cancer fighting compound that Zhao wanted to bring back to China.

In March 2013, Zhao was arrested and in possession of 384 files on his personal computer related to Anderson's research. Among the files was an application to a Chinese foundation claiming Zhao found the C-25 compound and requesting funding for additional research. Zhao was convicted in August 2013 of one count of unauthorized access to a protected computer.

UNIVERSITY OF TENNESSEE

J. Reece Roth, a Professor Emeritus at the University of Tennessee and part owner and technology transfer consultant at Atmospheric Glow Technologies, Inc., engaged in a conspiracy to transmit export-controlled technical data. The data was related to a restricted United States Air Force contract to develop plasma actuators for a munitions-type unmanned aerial vehicle. The indictment alleged Roth did not obtain permission to take the sensitive documents to China and lied to the Defense Department about his employment of a Chinese foreign national and an Iranian foreign national.

The trial started August 25, 2008, and on September 3, 2008, a federal jury in Knoxville convicted Roth of arms export charges. Roth was found guilty of conspiracy to violate the Arms Export Control Act, together with 15 separate illegal exports of military technical information. In July 2009, Roth was sentenced to four years in prison and two years probation.

PROTECTING YOUR ORGANIZATION

Suggestions to protect information from theft include the following:

- Identify information critical to your research/contracts.
- Train researchers/students on how to protect critical information from unauthorized disclosure.
- Institute physical/electronic access controls.
- Recognize and report suspicious activity to your local FBI Field Office or US Embassy.

PROTECTING YOUR PEOPLE

Suggestions to protect people from information theft include the following:

- Be cautious of people who show undue interest in your personal or family background, your research area, and your future career plans.
- Be cautious of people who offer "free favors," particularly those involving government processes such as issuing visas and residence permits.
- Minimize personal information that you reveal about yourself, particularly online through social media.
- Minimize your contact with foreigners who have questionable government or criminal affiliations.
- Report suspicious activity to your local FBI Field Office, US Embassy, or Consulate.

References

1. FBI; Insider Threat Brochure; http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat

2. FBI Internet Social Networking Risks; http://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks

3. FBI Visitors: Risks & Mitigations; http://www.fbi.gov/about-us/investigate/counterintelligence/risks-mitigations-of-visitors

4. FBI; Higher Education and National Security: The Targeting of Sensitive, Proprietary and Classified Information on Campuses of Higher Education; April 2011; http://www.fbi.gov/about-us/investigate/counterintelligence/higher-education-and-national-security

5. DSS; Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting; www.dss.mil/documents/ci/2014UnclassTrends.PDF

6. Washingtonian; Mole in Training: How China Tried to Infiltrate the CIA; 7 Jun 2012; http://www.washingtonian.com/articles/people/chinas-mole-in-training/

7. Bloomberg Business; Why The Professor Went to Prison; 1 Nov 2012; http://www.bloomberg.com/bw/articles/2012-11-01/why-the-professor-went-to-prison

8. Fox News; Man accused of “economic espionage” pleads guilty to lesser charge; 10 Jul 2013; http://www.fox6now.com/2013/07/10/man-accused-of-economic-espionage-pleads-guilty-to-lesser-charge/