FEDERAL BUREAU OF INVESTIGATION

CASE EXAMPLE: RESEARCH PARTNERSHIPS

CHINESE ENGINEER'S TARGETING OF HIGHLY SENSITIVE DEFENSE MATERIALS

A Chinese citizen and lawful permanent resident of the United States worked as a senior engineer and scientist at a U.S. company, working on engines used by the U.S. Air Force's F-22 and F-35 fighter aircraft. The Chinese citizen expressed to others his desire to return to China to advance his career and work on research projects related to his work at the U.S. company. The Chinese citizen then sought out research opportunities with several state-run institutions in China, including the Chinese Academy of Science (CAS) and an affiliate. Upon joining the CAS affiliate, the Chinese citizen agreed to provide the director and one of its recruiters with some of the U.S. company's documents to substantiate his credentials.

The U.S. Air Force declared the documents in the Chinese citizen's possession could have compromised broader research and development efforts

WORTH APPROXIMATELY $3.6 MILLION

A month after retirement from the U.S. company, the Chinese citizen traveled to China to begin work for the CAS affiliate. His CAS research plan stated China lacked the ability to process high-performance components, such as airplane wings and carrier aircraft tail hooks, as a result of its technology embargo. The Chinese citizen claimed by using Western companies' technology, his research project would increase China's independent ability, efficiency, and quality in key component manufacturing. He took with him to China his laptop and an external hard drive containing a significant amount of the U.S. company's highly sensitive, proprietary, and export-controlled materials—including data from projects outside his scope or access.

Upon his return to the United States from China, the Chinese citizen was found in possession of several suspicious documents containing Chinese characters and $10,000 in cash. Weeks later, he tried departing the United States for China with export-controlled and proprietary documents. The documents contained information on the U.S. Air Force's Metal Affordability Initiative. The U.S. Air Force declared the documents in the Chinese citizen's possession could have compromised broader research and development efforts worth approximately $3.6 million.

Lessons Learned: Vulnerabilities and Indicators

- **EGO.** The Chinese citizen was willing to provide controlled information to unauthorized personnel in order to advance his own career.
- **DIVIDED LOYALTY TO A COUNTRY.** As a result of his desire to assist China, he was susceptible to being tasked by Chinese government agencies and state-owned enterprises.
- **LARGE AMOUNTS OF CASH.** Upon entering the United States from China, the Chinese citizen was carrying $10,000 in cash.
- **POSSESSED CONTROLLED MATERIAL.** The Chinese citizen used a company-issued computer and hard drive to carry highly sensitive, proprietary, and export-controlled materials to China.
- **UNREPORTED FOREIGN CONTACT.** The Chinese citizen did not notify his employer about his foreign contact with officials at the Chinese Academy of Science.

RESEARCH PARTNERSHIP THREATS: VULNERABILITIES, INDICATORS, AND MITIGATION

VULNERABILITIES

Some circumstances that may render employees or companies more vulnerable to becoming research partnership threats:

- Large ego driving an employee's sense of happiness
- Divided loyalty to a country besides the United States
- Inadequate personnel policies and procedures
- Failure to conduct in-depth background checks of companies and employees
- Inadequate security procedures and training

INDICATORS

A research partnership threat typically demonstrates one or more of the following indicators:

- Working odd hours without authorization
- Taking sensitive material home without authorization
- Obtaining sensitive information without a need to know
- Inappropriately seeking sensitive information from others
- Bringing recording devices without approval into work areas
- Unnecessarily photocopying or downloading sensitive material
- Taking short trips to foreign countries for unexplained reasons
- Having unreported foreign contacts or conducting unreported foreign travel

MITIGATION

There are steps organizations may take to identify and deter potential research partnership threats. The FBI offers these for information, but each company must assess applicability in terms of its own policies, processes, and legal guidelines.

- Educate and regularly train employees on security policies and protocols.
- Ensure proprietary information is carefully protected.
- Employ appropriate screening processes to hire new employees.
- Develop strong risk management and compliance programs.
- Provide nonthreatening, convenient methods for employees to report suspicious behavior, and encourage such reporting.
- Monitor computer networks routinely for suspicious activities.
- Ensure physical security personnel and information technology security personnel have the tools they need.
- Create a program that regularly screens employees against insider risks.
- Conduct in-depth background checks on potential partners for associations with state-sponsored entities.
- Ensure retired, separated, or dismissed employees turn in all company-issued property.
- Evaluate the use of nondisclosure agreements and policies restricting the removal of company property.

CONTACT US:

For more information, contact your local field office at
https://www.fbi.gov/contact-us/field-offices