FEDERAL BUREAU OF INVESTIGATION

CASE EXAMPLE: NON-TRADITIONAL COLLECTOR

CHINESE CITIZEN'S THEFT OF WEAPONS TECHNOLOGY FOR CHINESE EMPLOYMENT OPPORTUNITY

A Chinese citizen was employed by a U.S. company that specializes in weapons, aerospace, communication, and electronic equipment development for U.S. government agencies. The Chinese citizen stole thousands of electronic files containing technical information about the company's weapons systems and then traveled to China with the files, where he delivered presentations about the technology at Chinese universities and at conferences organized by the Chinese government. The Chinese citizen sought to leverage the presentations to gain employment in China.

While in China, the Chinese citizen gave presentations at several universities, government research entities, and a government-organized conference. His presentations related to technology that he and his coworkers were developing for the U.S. Department of Defense. The Chinese citizen never sought the company's approval to deliver the presentation, which was contrary to the company's security rules. In fact, the Chinese citizen told one senior employee of the company before leaving for the trip that he was going to Chicago on vacation.

The Chinese citizen stole thousands of electronic files containing technical information about the company's weapons systems and then traveled to China with the files

When authorities stopped the Chinese citizen on his return trip to the United States, he was carrying a computer that had not been issued by his employer and contained information stolen from the U.S. company. A review of the computer's files indicated the information pertained to U.S. Munitions List items, which cannot be exported without a license—and the Chinese citizen did not possess a license. He previously received training from his employer on U.S. export-control laws and how they applied to the company's products.

The Chinese citizen was sentenced in 2013 to 70 months in prison for exporting sensitive U.S. military technology to China, stealing trade secrets, and lying to federal law enforcement.

Lessons Learned: Vulnerabilities and Indicators

- **DIVIDED LOYALTY TO A COUNTRY.** The Chinese citizen felt the U.S. company's information would benefit Chinese weapons and aerospace programs.
- **UNAUTHORIZED USE OF COMPANY INFORMATION.** The Chinese citizen leveraged presentations of sensitive U.S. company information to gain employment in China.
- **FALSIFIED TRAVEL ITINERARY.** When traveling to China for the presentations, the Chinese citizen told his employer he was traveling to Chicago.
- **UNDISCLOSED FOREIGN CONTACTS.** The Chinese citizen gave presentations at Chinese universities and government research entities.
- **ASKING FOR SENSITIVE MATERIAL WITHOUT AUTHORIZATION.** The Chinese citizen possessed sensitive U.S. company information on a non-work-issued computer.

NON-TRADITIONAL COLLECTORS: VULNERABILITIES, INDICATORS, AND MITIGATION

VULNERABILITIES

Some circumstances that may render employees more vulnerable to becoming non-traditional collector threats include:

- Loyalty to a foreign government
- The company's possession of technology or a product listed in China's Five-Year Plan
- Large ego as a result of expertise in a science and technology field of interest to foreign adversaries

INDICATORS

A non-traditional collector typically demonstrates one or more of the following indicators:

- Is sponsored by foreign country to study in the United States and then plans to return to his or her home nation with new technical knowledge
- Requests and/or obtains sensitive information without a need to know
- Inappropriately seeks sensitive information from others
- Brings recording devices without approval into work areas
- Unnecessarily photocopies or downloads sensitive material
- Takes short trips to foreign countries for unexplained reasons
- Displays unexplained affluence
- Takes numerous photos of booths and presentations at conferences
- Has unreported foreign contacts or conducts unreported foreign travel

MITIGATION

There are steps organizations may take to identify and deter potential insider 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.
- Provide nonthreatening, convenient methods for employees to report suspicious behavior, and encourage such reporting.
- Routinely monitor computer networks for suspicious activities.
- Ensure physical security personnel and information technology security personnel have the tools they need.
- Implement a continuous evaluation program to persistently screen onboard employees.
- Provide security personnel with full access to human resources data.
- Conduct exit interviews to identify potential high-risk employees.

CONTACT US:

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