FEDERAL BUREAU OF INVESTIGATION

CASE EXAMPLE: NON-TRADITIONAL COLLECTORS

CHINESE GOVERNMENT–SPONSORED THEFT OF U.S. PROPRIETARY INSULATION TECHNOLOGY

In November 2010, 58 people were killed and more than 70 injured in a Shanghai high-rise fire linked to faulty building materials—specifically, flammable building insulation. The ensuing public outrage prompted the Chinese government to invest millions in developing the domestic capability to produce better insulation. Two Chinese citizens used money from the Chinese government to acquire the insulation technology. The two Chinese citizens are assessed to be non-traditional collectors—individuals whose primary profession is not intelligence collection but who collect sensitive U.S. technologies and information on behalf of Chinese government entities.

If they had been successful,
THE U.S. COMPANY WOULD HAVE LOST MORE THAN $7 MILLION
it had invested in its research, development, and protection of the proprietary information

Instead of developing the insulation technology domestically, the two Chinese citizens sought to illegally acquire it from a U.S. company that produced the insulation technology. They published an advertisement in a U.S. newspaper canvassing for technical talent with experience at the U.S. company to lead the construction of a factory in Asia that would produce foam glass in direct competition with the U.S. company's proprietary insulation technology.

An individual responded to the ad and began corresponding and meeting with the pair. The two Chinese citizens offered to pay the individual to travel to China to consult on the production process. Though travel to China did not occur, the individual met with the two Chinese citizens to discuss details of the deal, indicating he would have to steal the insulation production and engineering documents. When the three met the next day, the individual showed the two Chinese citizens fake documents that resembled the U.S. company's proprietary materials, and they exchanged $100,000 for the purported trade secrets. The FBI subsequently arrested the two Chinese citizens, and they pleaded guilty to participating in a conspiracy to steal trade secrets. If they had been successful, the U.S. company would have lost more than $7 million it had invested in its research, development, and protection of the proprietary information.

Lessons Learned: Vulnerabilities and Indicators

- **FINANCIAL MOTIVATION.** The individual offered $100,000 for trade secrets.
- **FOREIGN PAYMENT AND TRAVEL.** The two Chinese citizens offered to pay the individual to travel to China to consult on the production process.
- **REQUESTS OF ILLEGAL ACTIVITY.** The individual was instructed to steal the insulation production and engineering documents.
- **ADVERTISEMENT CANVASSING FOR SPECIFIC EXPERTS.** The foreign company canvassed in a U.S. newspaper for technical talent with experience at the U.S. company to lead the construction of a factory in Asia.

NON-TRADITIONAL COLLECTION THREATS: VULNERABILITIES, INDICATORS, AND MITIGATION

VULNERABILITIES

Some circumstances that may render employees more vulnerable to becoming a non-traditional collector threat:

- Loyalty to a foreign government
- A company's possession or manufature of a technology or 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
- Financial distress or interest in financial incentives

INDICATORS

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

- Is sponsored by a foreign country to study or work 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 non-traditional collector 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 information technology and physical security personnel have the tools they need to share information.
- Create a program that regularly screens employees against insider risks.
- Provide security personnel with full access to human resources data.
- Conduct exit interviews to identify potential high-risk employees (such as terminated employees and retired employees with insider threat indicators).
- 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