FEDERAL BUREAU OF INVESTIGATION

CASE EXAMPLE: INSIDER THREAT AND NON-TRADITIONAL COLLECTION

CHINESE CITIZEN'S THEFT OF PROPRIETARY CORN SEEDS TO FULFILL CHINA'S DEVELOPMENT GOALS

A Chinese citizen was sentenced to three years in prison for conspiracy to steal trade secrets from U.S. agriculture companies. The Chinese citizen and five others participated in the theft of inbred corn seeds from fields the companies owned, with the aim of shipping them to a Chinese company. The seeds the Chinese citizen and his co-conspirators targeted were genetically modified to be stronger and enhance desirable traits, such as resistance to pests and drought. The Chinese citizen is assessed to be a non-traditional collector—an individual whose primary profession is not intelligence collection but who collects sensitive U.S. technologies and information on behalf of Chinese government entities.

Developing a single inbred seed can cost

$30–$40 MILLION

in laboratory testing and can take over seven years to develop

The Chinese citizen is also the U.S.-based director of a Chinese company that sold seeds through its subsidiary company. Both companies received favorable treatment from the Chinese government as National Key Dragon Head Enterprises—a designation China bestows on select private companies to recognize the significant role they play in promoting China's modernization and development goals.

A U.S. company informed the FBI it had observed the Chinese citizen digging up corn seeds from one of its farms the previous year. The FBI learned separately a sheriff's deputy had observed the Chinese citizen and two others acting suspiciously at a different farm. In addition, during a visit to another seed producer, the FBI learned company representatives had recently met with the Chinese citizen during a business trip to China. Moreover, the Chinese citizen had visited agriculture supply stores and purchased the U.S. company's seeds without signing the required contracts to purchase the seeds. Once they had acquired the seeds, the Chinese citizen and his co-conspirators attempted to transport them to China by mail and by concealing them in luggage leaving the United States by airplane and car. Conversations between the colleagues revealed they knew what they were doing was illegal. Although the Chinese citizen was sentenced to three years in prison, the U.S. company estimated the theft would result in the loss of five to eight years of research and at least $30 million.

CONTACT US:

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

Lessons Learned: Vulnerabilities and Indicators

- **UNAUTHORIZED ACCESS.** The Chinese citizen was observed digging up corn seeds from one of the farms.
- **SUSPICIOUS ACTIVITY.** A field manager noticed the Chinese citizen and two others acting suspiciously at different farms.
- **BYPASSING REGULATIONS AND POLICIES.** The Chinese citizen purchased the U.S. company's seeds without signing the required contracts.
- **TAKING SENSITIVE MATERIAL WITHOUT AUTHORIZATION.** Once the Chinese citizen acquired the seeds, he and his co-conspirators attempted to transport them to China by concealing them in luggage.

NON-TRADITIONAL COLLECTION THREATS: 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.