FEDERAL BUREAU OF INVESTIGATION

CASE EXAMPLE: FRONT COMPANIES

CHINESE CITIZEN'S TARGETING OF FORMER EMPLOYEES TO ACQUIRE CHEMICAL REFINEMENT PROCESS

A Chinese citizen used his U.S. company to sell stolen trade secrets to Chinese state-owned companies. China's State Council directed him to help advance China's business development priorities by targeting a chemical refinement process that could produce dual-use materials with military and aerospace applications. The Chinese government identified the development of chloride-route titanium dioxide (TiO_2) production capabilities as a priority. To achieve that goal, companies controlled by the Chinese government conspired to illegally obtain TiO_2 technology, which had been researched and developed over many years by a U.S. company.

THE U.S. COMPANY LOST ITS TRADE SECRETS AND PROPRIETARY INFORMATION. THE COST OF THE STOLEN SECRETS LIKELY TOTALED HUNDREDS OF MILLIONS OF DOLLARS.

The Chinese citizen targeted the U.S. company by assembling a team previously employed by the same U.S. company. The former employees provided proprietary information, including blueprints of buildings, chemical compositions, schematics, and photographs of equipment, temperature data, and pipelines. The Chinese citizen used a variety of techniques to elicit information from the former employees, exploiting their bitterness toward the U.S. company and flattering their egos with attention, presents, and offers to pay for personal expenses. After every gift or compliment, the Chinese citizen asked for information about the chemical process. Eventually, the Chinese citizen collected enough information from the former employees to be able to claim in a bid to a Chinese company that he had replicated the chemical refinement process.

To avoid arousing suspicion in the United States, the Chinese citizen hid his significant income from the Chinese company, lived a modest life, and falsified his financial records so it appeared he and his business earned less than they actually did—and even filed for bankruptcy. The Chinese citizen was found guilty of economic espionage and sentenced to the maximum 15 years in prison. Although he also had to forfeit $27.8 million in illegal profits and pay $511,667 in restitution, the U.S. company lost its trade secrets and proprietary information. The U.S. company informed the court that it could not determine lost profits because the stolen technology had not yet been used but that the cost of the stolen secrets likely totaled "hundreds of millions of dollars."

CONTACT US:

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

Lessons Learned: Vulnerabilities and Indicators

DISCONTENTMENT AND DISGRUNTLEMENT. The Chinese citizen targeted disgruntled former employees to steal information he otherwise could not obtain.

EGO. The Chinese citizen used flattery, deception, and financial compensation to recruit the former employees to his company.

DIRECTION BY A FOREIGN ENTITY. The Chinese citizen's U.S.-based company received direction and funding from China's State Council to obtain TiO_2.

FRONT COMPANY THREATS: VULNERABILITIES, INDICATORS, AND MITIGATION

VULNERABILITIES

Some circumstances that may render organizations more vulnerable to becoming front company victims include:

- Financial struggles within the company
- Inadequate personnel policies and procedures
- Failure to conduct in-depth background checks of companies and employee
- Inadequate security training and procedures in place

INDICATORS

A front company threat typically demonstrates one or more of the following indicators:

- Formal connection to foreign state-run or state-supported development goal
- A foreign company with multiple name variations
- Funding provided by a foreign government entity
- Independent patent filing in foreign country without U.S. partners on jointly developed programs
- Acquisition of sensitive information without a need to know
- Use of offshore addresses for transshipment points
- A company website that is under construction for long periods of time
- Limited information on websites regarding the company
- No description of products
- Push for access to restricted programs not within the company's scope of work

MITIGATION

There are steps organizations may take to identify and deter potential front company incidents: 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.
- Ensure the company with which you plan to partner has been thoroughly researched.
- 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.
- Routinely monitor computer networks for suspicious activities.
- Ensure information technology and physical 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 (such as terminated employees and retired employees with insider threat indicators).
- Evaluate the use of nondisclosure agreements and policies restricting the removal of company property.