FEDERAL BUREAU OF INVESTIGATION

CASE EXAMPLE: JOINT VENTURES

CHINESE COMPANY'S EXPLOITATION OF COLLABORATION TO STEAL PROPRIETARY PRODUCT

A Chinese telecommunications company collaborated with a major U.S. telecommunications company on research to increase the quality of both corporations' products. As part of the agreement, the Chinese company's employees were given access to the U.S. company's development laboratories. To protect its projects, the U.S. company established privacy and access restrictions, including security clearances, escort policies, and security surveillance.

The U.S. company claimed it suffered DAMAGES AND LOSSES TOTALING TENS OF MILLIONS OF DOLLARS, and the Chinese company earned hundreds of millions of dollars in profits from its illegal acquisition

The U.S. company gave two Chinese employees permission to access a laboratory housing an innovative and proprietary device. Disregarding the U.S. company's security protocols, the two Chinese employees allowed an unauthorized third employee to access the facility using their credentials. When the unauthorized access was discovered, the U.S. company removed the employee and forbade any future access to the laboratory. However, the following day, the two Chinese employees again granted access to the third employee, who took photographs of the U.S. company's proprietary device. The company again removed the employee from the laboratory, but the photographs were nevertheless transmitted to a Chinese research and development team.

Following this incident, the U.S. company banned all Chinese employees but one from the laboratory. The company required the remaining Chinese employee to be escorted at all times and recorded all activities on video. Despite these security measures, the Chinese employee removed parts from the device and placed them in a bag. Although the actions were captured on video and civil lawsuits were filed, the Chinese company learned enough of the technology to replicate the device.

NON-TRADITIONAL COLLECTOR:
An individual who is not operating on behalf of an intelligence service but who collects information from the United States and other foreign entities to support government-directed objectives.

The U.S. company claimed it suffered damages and losses totaling tens of millions of dollars, and the Chinese company earned hundreds of millions of dollars in profits from its theft.

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.** Two Chinese employees with access to the laboratory disregarded security protocols and allowed an unauthorized third employee access.
- **UNAUTHORIZED CAMERA.** The unauthorized third employee took photographs of proprietary devices. The photos were transmitted to a Chinese research and development team.
- **CONTINUOUS DISREGARD FOR SECURITY PROTOCOL.** Chinese employees provided access to other unauthorized employees on various occasions, even after being discovered multiple times.

JOINT VENTURE THREATS: VULNERABILITIES, INDICATORS, AND MITIGATION

VULNERABILITIES

Some circumstances that may render organizations more vulnerable to becoming joint venture victims include:

- Failure to negotiate strong terms of the joint venture
- Inadequate personnel policies and procedures
- Failure to conduct in-depth background checks of companies and employees
- Inadequate security training and procedures

INDICATORS

A joint venture threat typically demonstrates one or more of the following indicators:

- Formal connection by the partner company to a state-run or state-supported development goal
- Unauthorized access of proprietary information
- Funding provided by a foreign government entity
- Claims by the partner company in foreign patents that it was the sole inventor of products developed in a joint venture
- 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
- A potential partner's website with little information on the company
- Requests for information on sensitive programs not related to the joint venture

MITIGATION

There are steps organizations may take to identify and deter joint venture 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.
- 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.
- Monitor computer networks routinely for suspicious activities.
- Ensure both physical security and IT security personnel have the tools they need to safeguard your company.
- Negotiate the joint venture terms and penalize actions that contradict the agreement.
- Create a program that regularly screens employees against insider risks.
- Provide security personnel with full access to human resources data.