FEDERAL BUREAU OF INVESTIGATION

CASE EXAMPLE: INSIDER THREATS AND JOINT VENTURES

A U.S. SUPERCONDUCTOR COMPANY TARGETED FOR TRADE SECRETS

In 2005, a U.S. company initiated a business relationship with a Chinese wind turbine manufacturer. In addition to wind turbine design and engineering services, the U.S. company provided the Chinese company with proprietary software and equipment to regulate the flow of electricity between wind turbines and electrical grids. For many years, the relationship was highly profitable for the U.S. company, while the Chinese company developed into the largest wind turbine manufacturer in China and the second largest in the world.

More than 500 of the U.S. company's 700 employees lost their jobs within two years of the theft, its stock collapsed, AND IT LOST MORE THAN $800 MILLION IN BUSINESS

However, after signing $800 million in contracts with the U.S. company, the Chinese company severed its relationship and recruited an insider from the U.S. company to provide intellectual property to the Chinese company. A Serbian citizen who worked at a U.S. company subsidiary in Austria downloaded proprietary software onto a thumb drive and sent it to the Chinese company via his personal Gmail account in exchange for approximately $20,500. According to court records, the Serbian citizen covertly copied the proprietary software for the Chinese company, which no longer needed the U.S. company, and immediately severed the business relationship. In September 2011, the Serbian citizen confessed to the theft in an Austrian court.

The theft significantly impacted the U.S. company's operations because the Chinese company had accounted for roughly 80 percent of its business. More than 500 of the U.S. company's 700 employees lost their jobs within two years of the theft, its stock collapsed, and it lost more than $800 million in business.

Lessons Learned: Vulnerabilities and Indicators

- **DISCONTENTMENT AND DISGRUNTLEMENT.** The Serbian citizen was increasingly frustrated at work due to a demotion, according to his attorney.
- **FEELINGS OF UNAPPRECIATION.** The Serbian citizen felt more appreciated by the Chinese company, which offered him a multi-year contract at twice his current pay and an apartment, according to an attorney for a U.S. company.
- **FINANCIAL STRESS.** The Serbian citizen's personal financial situation was negatively impacted due to a recent divorce, according to his attorney.
- **LONELINESS.** At trial, the U.S. company alleged the Chinese company attempted to woo the Serbian with "all the human contact" he wanted, "in particular, female coworkers."
- **TAKING SENSITIVE MATERIAL WITHOUT AUTHORIZATION.** The Serbian citizen misused the U.S. company's computer system by downloading proprietary software onto a thumb drive, according to court records.

INSIDER THREATS: VULNERABILITIES, INDICATORS, AND MITIGATION

VULNERABILITIES

Some circumstances which may render employees more vulnerable to becoming insider threats:

- Financial stress
- Extramarital affairs
- Drug and/or alcohol abuse
- Loneliness
- Discontentment and disgruntlement
- Feelings of unappreciation
- Divided loyalty to a country besides the United States
- Disgruntlement to the point of wanting to retaliate against the government and/or company

INDICATORS

An insider threat typically demonstrates one or more of the following indicators:

- Working odd hours without authorization
- Taking sensitive material home without authorization
- Obtaining sensitive information without a need to know
- Inappropriately seeking sensitive information from others
- Bringing recording devices without approval into work areas
- Unnecessary photocopying or downloading of sensitive material
- Short trips to foreign countries for unexplained reasons
- Unexplained affluence
- Bragging about what they know
- Unreported foreign contacts or 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.
- Create a program that regularly screens employees against insider risks.
- Provide nonthreatening, convenient methods for employees to report suspicious behavior, and encourage such reporting.
- Routinely monitor computer networks for suspicious activities.
- Ensure both physical security and IT security personnel have the tools they need to safeguard your company.
- 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 non disclosure 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