2022 CHEMICAL SECURITY SUMMIT

August 23-25, 2022

#ChemicalSecurity

How Multi-National, Critical Infrastructure Organizations Protect Intellectual Property from Theft and Economic Espionage

DHS / CISA

CHEMICAL SECURITY SUMMIT

AUGUST 2022

Institute for Homeland Security
SAM HOUSTON STATE UNIVERSITY

Preventing International Theft or Economic Espionage Learning Objectives for Today

1. Understand the Scope of Risk for International Theft or Economic Espionage when Operating Critical Infrastructure Businesses Overseas
2. Be able to identify common strategies used for conducting Proprietary Information Theft and/or Economic Espionage
3. Be able to identify the primary global actors associated with Proprietary Information Theft and/or Economic Espionage
4. Be able to identify Strategies for proactively protecting sensitive or protected critical infrastructure information from International Theft or Economic Espionage in a physical or cyber environment
5. Be able to identify the Pre-incident Indicators of potential International Theft or Economic Espionage from “Insider Threats”
6. Understand how to detect pre-incident indicators of potential International Theft or Economic Espionage
7. Understand what steps to take if your organization suspects potential International Theft or Economic Espionage is being directed at them

Scope of the Problem

What's the Difference Between International Theft, Economic Espionage, and Espionage?

Why does it matter?

But, 'I'm not a target. We don't make any products for the military or national security, or that are cutting edge technology that will potentially change the future!'

What's the difference between Cyber Espionage, Cyber– Warfare, and Cyber Economic Espionage?

- Are they the same thing?

Scope of the Problem

Impact of Economic Espionage to Critical Infrastructure Companies

- Lost revenue – ($250 to $400 billion lost annually)
- FBI – cases increasing steadily since 2010; New case every 10 hours)
- Damaged Reputation – Lost Jobs – Lost Bonus Payments
- Lost R&D Investment – Kraft Foods Example
- Production Interruption - Reduced Labor Hour Productivity – Market Value
- Existential Threat to Critical Infrastructure Organization

Examples of Physical Theft / Espionage & Cyber Theft / Espionage

- **Physical:** Spot, Assess, Develop, Recruit, Exploit, Terminate
- **Cyber:** Spot, Assess, Develop Plan, Execute, Exploit Data Removal, Exposure?

Economic Espionage Strategies Differ by Culture and History

For Example - Intelligence Target: Analyze a Beautiful Beach along the Ocean!

France: Send a Submarine with Embarked Swimmers to dig / collect sand

Russia: Use Satellite surveillance to photograph and analyze the chemical signature of the beach

Israel: Infiltrate the beach life-guard service to collect samples of sand

China: Over the course of multiple years, send 5,000 tourists to sun-bathe on the beach by laying upon a Beach Towel – each tourist is instructed to gather one (1) grain of sand and bring it back to Beijing….And then…..

Where is Economic Espionage Most Common?

Top seven (7) nations for implementing economic espionage against US and other nations businesses operating in their country (nearly 80% of known incidents):

China, Japan, Israel, France, South Korea, Russia, Taiwan, and India

Countries who employ economic espionage in support of their nation's businesses:

Algeria, Armenia, Azerbaijan, Belarus, Cuba, Georgia, Iran, Iraq, Kazakhstan, Kyrgyzstan, Libya, Moldova, Pakistan, Syria, Turkmenistan, Ukraine, and Uzbekistan

Institute for Homeland Security
SAM HOUSTON STATE UNIVERSITY

Common Economic Espionage Tactics

Theft: Stealing information or products

Blackmail: using threat or intimidation to extort information

Mole planting: a double agent is embedded and gains the trust of a competing company

Eavesdropping: ranges from wiretapping phones to intercepting WIFI signals and emails.

Seduction: timeless technique using sexual offers to get information out of an individual.

Bribery: influence someone by offering money to gain information or prompt illegal action.

Foreign intelligence recruits: business intelligence agencies, such as Kroll, recruit former Cold War intelligence officers for commercial intelligence purposes.

Hiring competitors' employees: hiring away critical employees from a competitor.

Bogus job interviews: Fake interview of candidates solely for the purpose of collecting key information on the employer and their operations.

Common Economic Espionage Tactics

Bogus purchase negotiations: Companies pose as “buyers” in order to gain key information from a competitor.

Research under false pretenses: “Author” uses research paper as ruse to gain key information from a competitor.

Corporate communication intercepts: Intercepting telephone calls through public switch exchange.

Trade fair conversations: establishing a contact at trade fairs, particularly with experts having a high level of understanding of innovative technology.

Dumpster Diving: foraging for sensitive data or materials thrown into garbage.

Naturalized citizens: appealing to naturalized citizens to provide information for patriotic or loyalty reasons or threatening family members in the home country.

Repatriating naturalized citizens: lure naturalized citizens back to the home country to employ process and methods used by the foreign company.

Common Economic Espionage Tactics

Government debriefing: mandatory debriefing of citizens to acquire information upon return from a foreign country.

Dumpster diving: going through a competitor's trash to find key information.

Outsourcing/Delocalization: Foreign outsourcing can exploit methods, processes or information. Delocalizing under license often leads to a loss of data security in countries unencumbered by copyright or trademark laws.

Front companies and organizations: foreign competitors pose as software vendors or even nonprofit organizations to access a competitor's trade secrets.

Joint venture & bidding process: foreign purchasers may prompt companies to provide a great deal of data in the bidding process, compromising valuable proprietary information.

Close proximity: joint ventures and strategic alliances put unscrupulous personnel in close proximity with a firm's key personnel or technology.

Mergers & acquisitions: mergers and acquisitions often allow a new company to acquire certain technologies not in their prior possession.

Common Economic Espionage Tactics

Import-export front: import/export companies may be involved with illegal exporting of sensitive or illegal documents, data or other items in the country of export.

Altered products or false certifications: domestic companies serve as fronts for sending export-controlled products to an undisclosed end user by falsifying end-user certificates.

University research: spies placed in university research facilities by government intelligence services or by commercial competitors.

Negotiating: Buyers make excessive technology information demands during negotiations.

Third-party acquisition: Acquisition occurs to achieve a diversion or transfer of technology. Final recipients are embargoed / sanctioned individuals, businesses or countries that cannot otherwise obtain the technology.

Luggage or laptop theft: Foreign business traveler's briefcases and/or luggage in hotel rooms is searched for sensitive data or technology to be downloaded. Customs officials "seize" laptops or cell phones or tablets at a border entry point to covertly copy the contents.

Common Cyber Espionage Tactics

Exploiting Website / Browser Vulnerabilities

Spear Phishing to Escalate Network Privileges

Supply Chain Attacks on Primary Partners or through Joint Venture Partners

Malware, Trojans, Worms

Infecting Updates of Common 3rd Party Software Applications

Inserting keystroke monitors accessible by wireless or external port downloads

Copy computer files using miniature USB drives and pass them to other individuals, businesses or governments

Information scam requests for sensitive information, particularly via the internet using phishing, or Business Email Compromise, or Social Engineering, or Malware insertion, etc., focusing upon unsuspecting low or mid-level personnel

Methods to Protect against Economic Espionage

PLAN Strategy

"P" – **Prepare** by identifying the threat and the tactics used in each jurisdiction to access confidential data

"L" – **Learn** what trade secrets and sensitive or protected business data exists, where it's located in your business, how it is used within your critical infrastructure business, and the information's value to the organization

"A" – **Analyze** whether the data is currently protected and if so, is it sufficiently protected in accordance with the information's value to the company and its vulnerability to unauthorized access. Develop a risk-based plan to protect data from unauthorized access in the country or region you are operating business. Assess the security vulnerability of your employees, partners and key contractors as well

"N" - **Notify** employees of warning signs of international theft or economic espionage and establish multiple means of reporting indicators of concern. Implement systematic awareness training for executives and annually test procedures and processes for detecting, managing, responding to and reporting incidents of unauthorized data access with senior leadership from Legal, HR, CEO, IT, CISO, CSO, OPS, CorpCom using a TTX

Effective Strategies for Protecting Against Data Theft or Economic Espionage

Data / Document Classification Process

- Courts require reasonable steps to protect data – Protection needs to be clearly understood

Physical Access Controls and Cyber Controls– Clear segmentation of Access to Protected Files based upon employee, partners, contractors risk vulnerabilities

- Look for Abnormal file access Activities
- Require multi-factor Identification for IT network access
- Install security update patches for IT network; Institute network / digital security training from day 1
- Implement strong password management, network security audit and accountability performance measures
- Clear background investigations and update policies for employees and contractors
- Institute a defined employee termination process involving immediate IT / Physical access revocation and look-back period

Temporary Mobile Phones and Laptops or Tablets issued to Company Travelers to High Espionage Risk Nations, like China or Russia

Random Monitoring of Employee or Partners or trusted Contractors Access to Files and IT Networks; Alerts issued when employees access (or attempt to access) areas outside of Normal

Strategies for Protecting Against Data Theft or Economic Espionage

Mandate economic espionage security briefing for ALL travelers to high espionage threat countries

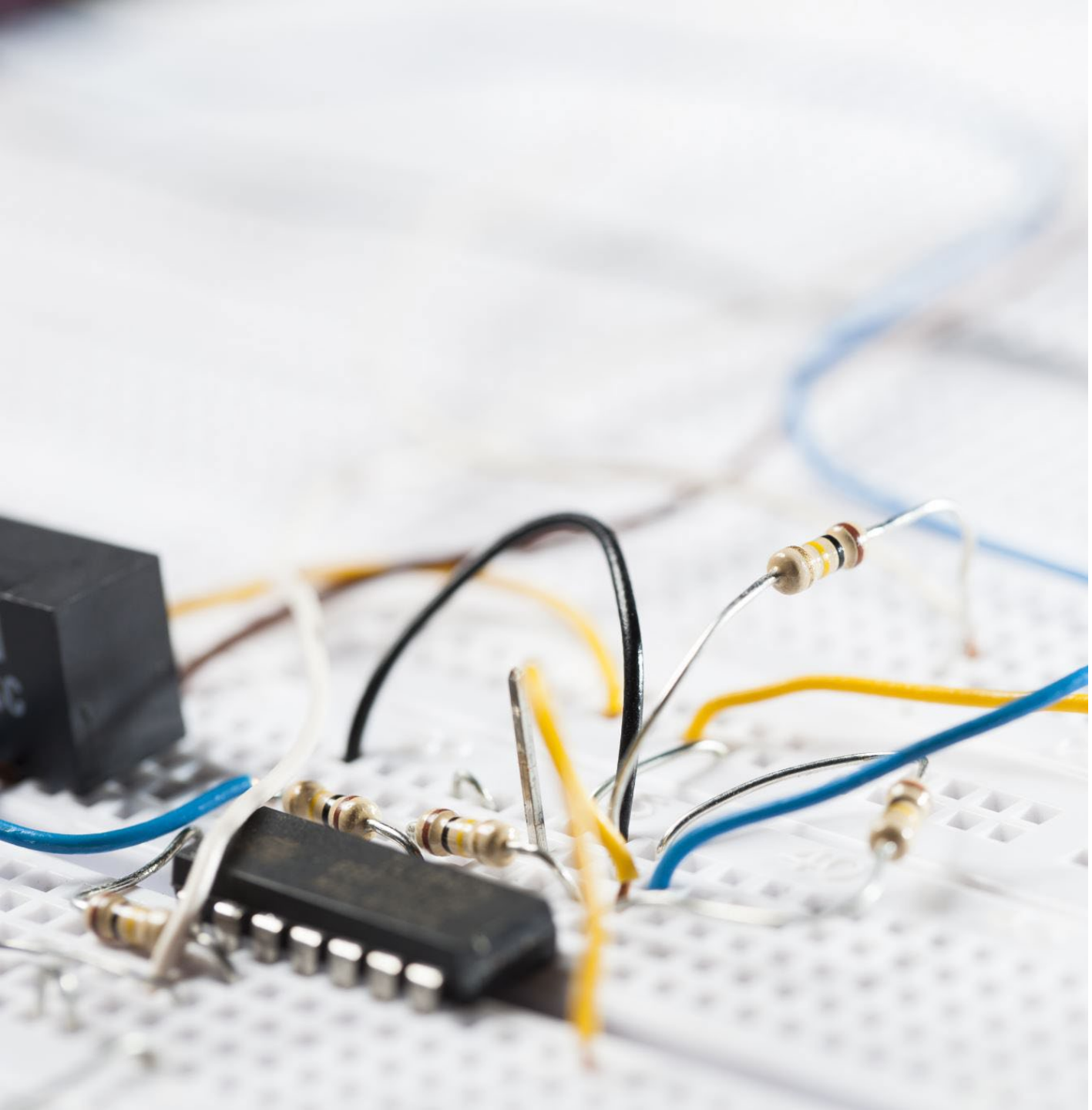
- Randomly debrief high-risk travelers (R&D, Manufacturing engineering / management, HR, Administrative and Personal Assistants to Senior Leadership, Senior IT Leadership, C-Suite Executives)

Employee background investigation to include indicators of Economic Espionage Connections

Know your Customer/Supplier/Vender/ Partner Due Diligence– Looking for connection to SOE or Government Officials

Security Awareness Training and Briefings (On-boarding and Case-study updates)

- Continuous Reinforcement of Message
- Computer Banner Messaging
- See “Something – Say Something” Program w/HR – Internal Audit; Ethics – Compliance Reporting Hotline
- Surveillance Detection & Awareness



What are Technical Security Counter-Measures (TSCM)?

- Effective Against “Insider Threat” Low Level Listening Devices
- Used to “Sweep” for Electronic Listening Devices aka: “bugs”
- Does not work well detecting sophisticated devices – particularly those which can power offer between transmissions

Who Conducts Economic Espionage or Theft of Data?

1. Foreign Government Employees
2. People Working at the Direction or Influence of Government Agencies
3. Critical Infrastructure Direct or Indirect Competitors
4. Private, 3rd Party Industrial Espionage Firms (Not Competitive Intelligence Firms which are researchers who collect and analyze legally available "open source" data of industry or company business operations analysis)
5. Insider Threat (Disgruntled Employees, Those seeking Vengeance or Career Advancement etc.)

#1 & #2 account for 36% of economic espionage

#5 accounts for 40% of economic espionage

What are Some Indicators of "Insider Threat" Economic Espionage?

- Unexplained changes in life-style
- Living beyond their financial means, with no explanation as to where the money is coming from
- Unexplained or unreported trips abroad
- Staying at the work-site late at night, or after-hours for no apparent reason
- Attempting to access physical or cyber locations in which they are not authorized
- Attempts to access IT files or networks that are not connected to the persons work duties

What are Some Indicators of "Insider Threat" Economic Espionage?

- Unexplained financial problems (gambling, drugs, alcohol, other addictions)
- Visible and persistent anger with the company, or certain leaders within the company due to a perceived wrong (i.e. passed over for promotion, transfer denied, poor performance evaluation, disrespected in group setting, etc.)
- Unexplained departures from work; unusual and unexpected decline in work performance
- Personality changes – now acting aloof, loner, morose, depressed, short tempered, on-edge, paranoid, etc.
- Unexplained support & admiration for a foreign culture, foreign company, government or leader – visits to that country

Is Protecting against Economic Espionage just a Corporate Security Responsibility?

Multi-Functional Responsibility – HR, CEO, Legal, Ethics-Compliance, Internal Audit, IT, CISO, CSO, CorpCom, Operations

All the above functions need to be Educated about the Threat, and its Risk to Critical Infrastructure, and that is a CISO / CSO role

Annually need to revalidate and test the organization's ability to detect, deter and manage a economic espionage or material theft or product counterfeiting, sabotage, or blackmail ransomware incident

Institute for Homeland Security
SAM HOUSTON STATE UNIVERSITY

Know the Tactics of the Prime Economic Espionage Threat

Thousand Talents Program part of the Belt and Road Initiative (as of 2020 already surpassed 10,000 members)

Overseas Student and Intern Debriefing Program, mandatory

National Law requires every Chinese citizen to collect and report to government any information about foreign business processes, procedures, technology, engineering and/or product data

Those who steal sensitive, proprietary foreign business data and transmits it to Chinese business competitors will not be prosecuted by China authorities

Know your Partner – State Owned Enterprise (SOE) or Government / Military / Militia Connections?

- Know your Supplier - State owned Enterprise (SOE) or Government / Military / Militia Connections?
- Know Your Employees - State owned Enterprise (SOE) or Government / Military / Militia Connection?

Know the Tactics of the Prime Economic Espionage Threat

Primary Espionage / Theft Targets: Energy, Technical, Chemical, Manufacturing

Economic Espionage Strategy of China Intelligence Services

1. Use China intelligence personnel to recruit foreign citizens with access to economic information needed by China industry
2. Use non-traditional collectors such as students, interns, academics to gain access to sensitive economic information which they can collect for China industry
3. Cyber-attacks to access foreign IT networks and steal economic information for China industry
4. Target corporate 3rd party law firms providing patent, trademark, and data protection & privacy services

Knowledge Test (True or False)

1. The “Thousand Talents Program”, a component of the Belt and Road geo-political Initiative, has been an effective Economic Espionage tactic employed by China?
2. The primary locations that employ Economic Espionage techniques in support of their nations industry are India, France, Israel, Taiwan, Russia, China, South Korea?
3. Cyber-warfare, Cyber-Espionage and Ransomware are synonyms, with each having the same Economic Espionage purpose?
4. Economic Espionage has been declining over the past decade in response to new law enforcement cooperation with high espionage threat foreign governments?
5. Technical Security Counter-Measures are a particularly effective means of detecting covert listening devices placed in support of Economic Espionage?