Student Guide

Sensitizing Facility Employees to CI Concerns

Course Introduction

Course Introduction

Course Overview

Counterintelligence (CI) is a fundamental and critical component of any successful security program. But to be successful, CI needs to be ingrained into a facility's culture. Employee awareness is central to a successful CI program. Facility Security Officers (FSOs) play an important role in helping facility employees understand they are the first line of defense against the adversaries that may threaten their facility and its technology.

Welcome to the Sensitizing Facility Employees to CI Concerns course.

Course Objectives

Here are the course objectives. Take a moment to review them.

- Identify the key employee groups at your facility most likely to be targeted by an adversary attempting to gain information:
    - Identify the vulnerability of each of these groups
    - Identify the kinds of contacts these groups are likely to experience
- Identify ways to promote employee awareness and reporting of issues of CI concern

Student Guide

Sensitizing Facility Employees to CI Concerns

Lesson 1: Identifying Employee Targets within Your Facility

Introduction

Objectives

As an FSO, it is your duty to understand the threats your facility and its employees may encounter.

The success of your organization's security and counterintelligence programs depends on your ability to identify *what* must be protected and *what*—or *who*—may threaten it.

Understanding how key employee groups may be targeted, their vulnerabilities, and the types of contacts they may experience will help you protect them. And in turn, help them protect themselves.

Here are the lesson objectives:

- Identify the key employee groups at your facility most likely to be targeted by an adversary attempting to gain information:
    - Identify the vulnerability of each of these groups
    - Identify the kinds of contacts these groups are likely to experience

CI and Industry Targets

What Are We Protecting?

Your employees have access to sensitive information in the course of their daily work. Because of this, THEY themselves are targets of adversaries trying to gain unauthorized access. One of your responsibilities as an FSO is to help employees understand that adversaries will approach them for what they know and for what they have access to.

So what, exactly, should they be looking out for? Adversaries target a facility's people, its systems and technology, and its information. Employees should understand that a single piece of information - classified or not - may not be of critical importance alone, but when put together with other pieces of information, may reveal sensitive, or even classified, information. For this reason, employees need to protect not only classified information, but also controlled unclassified information, business proprietary information, and intellectual property. The loss of *any* of these directly impacts your company's economic viability and national security.

So as an FSO, it is your responsibility to ensure your employees understand this and are aware of the ways adversaries may approach them. They also need to know what they should do if that happens.

Your CI program will succeed only if it has a knowledgeable and alert workforce acting in support of it.

Who May Be a Target?

Adversaries target employees who perform a variety of specific functions – and they target them in different ways.

As an FSO, you need to know who these employee groups are, so you can make them aware of potential contact from adversaries. The better prepared they are, the lower the chance of compromising your facility's sensitive information.

Human Resources

Human resources personnel are the gateway to your facility. They are appealing targets for adversaries because of their access to personnel information *and* because they play an important role in the hiring process.

Human resources is the only activity within an organization with exposure to an employee from pre-hiring, during employment, and through post resignation or post retirement.

Common collection methods adversaries use when approaching HR personnel are to pose as interns looking for a temporary position, or to seek to come in as a new hire.

HR personnel can be an important part of your CI program. Their access to personnel information equips them to help spot the warning signs of an insider threat. You can learn more about recognizing insider threats in the DSS web-based training *Insider Threat Awareness*, available through CDSE's Security, Training, Education and Professionalization Portal (STEPP.)

HR personnel must be aware of all collection methods, but especially:

- Academic solicitation (interns)
- Seeking employment
- Insider threat

Information Technology

Information Technology (IT) personnel are the electronic gatekeepers for your facility. They are appealing targets for adversaries because of their access to the facility's network and information systems. And the personally identifiable information (PII) of your employees likely resides on those networks.

IT personnel should be central to your CI program. Their access to system and network activity equips them to notice anomalies and spot cyber attacks. They should especially pay attention to suspicious internet and network activity which may indicate either intrusions or inappropriate insider activities.

IT personnel must be aware of all collection methods, but especially:

- Cyber threat (suspicious Internet and network activity)

Business Development

Business development personnel, which includes marketing and sales, are essential to your company's growth. But they are appealing targets for adversaries because of their access to your company's sensitive and proprietary information *and* because they play a key role in determining who your organization will conduct business with.

Adversaries may use many methods when approaching business development personnel. Personnel need to be aware of this and pay careful attention to requests for information and attempted acquisition of technology.

Business development personnel also should know the signs of adversary targeting when looking at joint ventures; Foreign Ownership, Control or Influence (FOCI) decisions; and any ventures relating to the Committee on Foreign Investment in the U.S. (CFIUS.) They must also be knowledgeable of International Traffic in Arms Regulations (ITAR) and common indicators that a potential buyer is attempting to illegally purchase technology which is export controlled. Finally, personnel also must understand the risks that may be present at conferences and trade shows.

Business development personnel should be an important part of your CI program. Their access to those seeking to do business with your organization not only equips them to identify potential targeting early, but it also allows them to identify *what* is being targeted.

Business development personnel must be aware of all collection methods, but especially:

- Request for information
- Solicitation and marketing of services
- Attempted acquisition of technology
- Elicitation
- Joint ventures
- Foreign Ownership, Control or Influence (FOCI) decisions
- Committee on Foreign Investment in the U.S. (CFIUS) ventures
- Potential International Traffic in Arms Regulations (ITAR) violations
- Illegal purchase of export-controlled items or technology
- Conferences and trade shows
    - Theft
    - Unapproved photography
    - Unapproved acquisition of samples

Engineers and Research and Development (R&D)

Engineers and research and development (R&D) personnel need to be aware that they are targets due to their knowledge of and access to blueprints, diagrams, and other technical information.

Adversaries may approach them in a number of ways. They must be aware of the risks associated with conferences and trade shows. They should pay close attention to any academic solicitations they receive. They also need to be aware of anyone looking to exploit relationships to gain access to information and technology.

Engineers and R&D personnel are an important component of your CI program. They can help identify specifically what is being targeted based on the inquiries and solicitations they receive.

Engineers and R&D personnel must be aware of all collection methods, but especially:

- Conferences and trade shows
- Academic solicitation
- Exploiting relationships

Manufacturing and Direct Labor

Manufacturing and direct labor personnel are targets for adversaries because of their access to the facility and its technology, processes, and end products

Common collection methods adversaries use when approaching these personnel include exploiting relationships, relationships they may cultivate over time, without the employee ever knowing the end goal.

You can help facility personnel be aware of this and make sure keep an eye out for any suspicious contacts.

Manufacturing and direct labor personnel must be aware of all collection methods, but especially:

- Exploitation of relationships
- Suspicious contacts

Purchasing

Individuals working in purchasing are targets for adversaries because of their access to the organization's supply chain. Adversaries often seek to disrupt or sabotage supply chains. Purchasing personnel must be aware of the specific risks to your organization's supply chain. They should pay special attention to any suspicious interactions with vendors and be aware of potential risks with Freight Forwarders used for shipping.

Purchasing personnel must be aware of all collection methods, but especially:

- Risks to the supply chain
- Vendor contacts
- Freight forwarders

Facilities Management

Facilities management personnel are your organization's eyes and ears. They are appealing targets for adversaries because of their physical access to your facility – and thus, to all of the information, technology, and personnel within it.

Common collection methods adversaries use when approaching facilities management personnel are to pose as a vendor – such as those working with the facility's vending machines or heating and plumbing systems.

Adversaries may also seek to exploit an existing relationship to gain access or may make unusual requests for access to facilities or systems.

Facilities management personnel must be aware of all collection methods, but especially:

- Suspicious contacts with vendors
- Exploitation of relationships
- Unusual requests for access to facilities or systems

Employees Traveling Abroad

Because your facility's employees have access to sensitive information, it is especially important for any employee who travels outside of the U.S. to be aware of the risks associated with foreign travel.

As an FSO, it is your responsibility to provide them with a foreign travel briefing before they go to increase their awareness of potential targeting and to provide information on current travel warnings and alerts.

In addition, when an employee *returns* from foreign travel, it is important to conduct a foreign travel *de*brief.

You can learn specifics information about CI foreign travel briefings in the DSS web-based training Short *CI Foreign Travel Briefing*, available through CDSE's Security, Training, Education and Professionalization Portal (STEPP.)

Targeting Methods

Common Targeting Methods

How do adversaries attempt to obtain information?

The most common foreign collection methods, used in over 80% of targeting cases are:

- Cyber attacks
- Attempts to acquire technology
- Academic solicitation
- Requests for information

As an FSO, you can help employees recognize these methods so they do not fall victim to them.

Cyber Attacks

Attempts to carry out intrusions into cleared contractor networks and exfiltrate protected information

Examples include, but are not limited to:

- Cyber intrusion
- Viruses
- Malware
- Backdoor attacks
- Acquisition of user names and passwords
- Attempts to acquire technology
- Academic solicitation
- Requests for information
- Social engineering

Attempted acquisition of technology

Attempts to acquire protected information in the form of controlled technologies via direct purchase of firms or agency of front companies or third countries

Examples include, but are not limited to, attempted purchases of:

- Equipment
- Diagrams
- Schematics
- Plans
- Spec sheets

Academic solicitation

Attempts to acquire information and technology via academic request, including all expenses paid invitations to travel and present at seminars and conferences in foreign countries

Examples include, but are not limited to, requests for or arrangement of:

- Peer or scientific board reviews of academic papers or presentations
- Requests to study or consult with faculty members
- Applications for admission into academic institutions, departments, majors, or programs, as faculty members, students, fellows, or employees

Request for information

Attempts to collect protected information via phone, email, or web card approaches

Examples include, but are not limited to, requests under the guise of

- Price quotes
- Marketing surveys
- Other direct and indirect efforts
- Social engineering

Other Targeting Methods

Other targeting methods include:

Solicitation or Marketing of Services

Attempts by foreign entities to establish a connection with a cleared contractor vulnerable to the extraction of protected information

Examples include, but are not limited to:

- Sales
- Representation
- Agency offers
- Response to tenders for technical or business services

Foreign Visit

Attempts to gain access to and collect protected information that goes beyond that permitted and intended for sharing

Examples include, but are not limited to:

- Pre-arranged visits by foreign contingents
- Unannounced visits
- On site foreign technical or liaison representatives to large acquisition programs who, while traveling abroad or traveling to foreign countries, do not wear uniforms on site and cannot be distinguished from U.S. personnel

Seeking Employment

Attempts to introduce persons who, wittingly or unwittingly, would thereby gain access to protected information that could prove useful to agencies of a foreign government

Examples include, but are not limited to:

- Résumé submissions
- Applications
- References

Exploitation of Relationships

Attempts to play upon existing legitimate or ostensibly innocuous relationships to gain unauthorized access

Examples include, but are not limited to, establishing connections via:

- Joint ventures
- Official agreements
- Foreign military sales
- Business arrangements
- Cultural commonality

Surveillance

Attempts to comprise systematic observation of equipment, facilities, sites, or personnel

Examples include, but are not limited to:

- Visual
- Aural
- Electronic
- Photographic

Criminal Activities

Attempts to acquire protected information with no pretense or plausibility of legitimate acquisition

- Example: Theft

Search and Seizure

Attempts to temporarily take from or permanently dispossess someone of property or restrict his/her freedom of movement, primarily when traveling abroad

Examples include, but are not limited to, physical searches of and/or tampering with:

- People
- Environments
- Property

Open Source Collection

Attempts to gather information that is legally available either free or for a fee, including but is not limited to obtaining information from:

- Press releases
- News articles
- Websites
- Advertising and promotional brochures, etc.

Review Activities

Question 1

You learn from a security bulletin that a foreign country is using university students to gain entry into companies in your industry. Which group should you alert first?

Select the best response.

- ○ Human Resources
- ○ Information Technology
- ○ Business Development
- ○ Engineers and Research & Development

Question 2

There is an increase in attempts from foreign entities to purchase export-controlled technology, including technology your facility develops. Who should you alert?

Select the best response.

- ○ Human Resources
- ○ Information Technology
- ○ Business Development
- ○ Engineers and Research & Development

Question 3

You learn of a threat from a business competitor to steal blueprints and schematics. Who should you alert?

Select the best response.

- ○ Human Resources
- ○ Information Technology
- ○ Business Development
- ○ Engineers and Research & Development

Question 4

There is an increase in cyber attacks against companies in your industry. Who should you alert?

Select the best response.

- ○ Human Resources
- ○ Information Technology
- ○ Business Development
- ○ Engineers and Research & Development

Answer Key

Question 1

You learn from a security bulletin that a foreign country is using university students to gain entry into companies in your industry. Which group should you alert first?

- ◉ Human Resources
- ○ Information Technology
- ○ Business Development
- ○ Engineers and Research & Development

Question 2

There is an increase in attempts from foreign entities to purchase export-controlled technology, including technology your facility develops. Who should you alert?

- ○ Human Resources
- ○ Information Technology
- ◉ Business Development
- ○ Engineers and Research & Development

Question 3

You learn of a threat from a business competitor to steal blueprints and schematics. Who should you alert?

- ○ Human Resources
- ○ Information Technology
- ○ Business Development
- ◉ Engineers and Research & Development

Question 4

There is an increase in cyber attacks against companies in your industry. Who should you alert?

- ○ Human Resources
- ◉ Information Technology
- ○ Business Development
- ○ Engineers and Research & Development

Student Guide

Sensitizing Facility Employees to CI Concerns

Lesson 2: Building a Culture of CI Awareness among Employees

Introduction

Objectives

The success of your facility's counterintelligence program relies in large part upon its employees. Are they aware of the potential threats against your facility? If confronted with such a threat, would they recognize it? Would they know what to do? Your facility's security and continued viability--and our national security--rely upon your ability to answer "Yes" to these questions.

Here is the lesson objective:

- Identify ways to promote employee awareness and reporting of issues of CI concern

Communicating with Employees

Communication Strategies

As an FSO, you are responsible for creating a culture of CI awareness within your organization. Communication is an essential part of building that culture.

To be effective, communication should not be a one-time event. It should be a continuous process that reinforces key messages over time.

One strategy might be to communicate information tailored to specific employee groups in different forms and at different times. This will enable you to provide a clear, focused message directly to those people to whom it is most relevant.

Another strong theme to emphasize to employees is that they truly are the first line of defense in protecting against threats by recognizing and reporting suspicious activity.

Communication Methods

As an FSO, there are a variety of methods you can use to promote CI awareness.

You can share actual examples of suspicious activity targeting your facility – for example, emails, phone inquiries, and other contacts that employees received.

Another method is to periodically share relevant portions of the DSS *Targeting Trends* report and other threat reports, as well as any security reports and bulletins that apply to your industry.

You can also call upon your local DSS, FBI, and law enforcement contacts to brief employees on the specific threats to your facility.

Another effective communication method is to make CI and reporting responsibility reminders visible throughout the facility. You can accomplish this in many ways; for example:

- Creating bulletin boards specifically for CI and security topics
- Placing CI pamphlets, brochures, and posters in company high traffic areas
- Sending regular electronic reminders to employees

If the employees in your facility speak multiple languages, remember to communicate messages in those languages.

The success of your CI program depends on your facility's employees' ability to recognize and report threats. Layering and varying the messages employees receive will help them recognize a threat if and when they encounter one.

Encouraging Employee Reporting

Importance of Reporting

As an FSO, it is important to emphasize to facility employees how critical it is for them to report all suspicious activity or contacts they observe. It may be helpful to remind them that the best way to defeat the threat is to report the threat. Reporting helps protect not only your organization, but also national security.

It is important for employees to know that reporting does not reflect negatively on your facility. In fact, DSS expects companies, especially those in certain industries, to report suspicious activity, and to report often!

To help employees understand this, you can educate them on how DSS uses the information provided by reporting and how it will help your organization.

When your facility submits a report, DSS evaluates and screens it. Depending on the specific threat and its seriousness, this analysis will take place at various levels.

The analysis of all of the reports DSS gathers from its industry partners over time makes it possible for it to develop current, specific threat information. DSS can then, in turn, provide that information *back* to industry, which better equips companies like yours to face new and emerging threats.

Reporting Guidelines

Employees should know that contractors are required to report certain events and incidents. DoD 5220.22-M, the National Industrial Security Program Operating Manual (NISPOM) outlines the reporting requirements that apply to industry.

While employees should know to report to their FSO, it can be helpful for them to know where the information is ultimately reported.

FSOs report:

- Criminal activity within an organization to local law enforcement and DSS
- Suspected espionage, sabotage, terrorism, or subversive activities to the FBI with a copy to DSS
- Issues related to national security to DSS
- Suspected malicious cyber activity to both the FBI and DSS

As an FSO, you must enter adverse information into the Joint Personnel Adjudication System (JPAS.)

Finally, when considering whether or not to report an incident or event, always report to DSS if there is any doubt. It can be helpful to share examples of reportable events and incidents with employees.

Examples of Reportable Events or Behaviors

The following is not intended to be an exhaustive list. When in doubt, report an event or behavior.

Recruitment

Report events or behaviors including, but not limited to:

- Contact with an individual associated with a foreign intelligence, security, or terrorist organization
- Failure to report an offer of financial assistance by a foreign national other than close family
- Failure to report a request for classified or unclassified information outside official channels
- Engaging in illegal activity or a request to do so

Information Collection

Report events or behaviors including, but not limited to:

- Requests to obtain classified or protected information without authorization
- Requests for witness signatures for destruction of classified information when destruction was not witnessed
- Operating unauthorized cameras, recording devices, computers, or modems in areas where classified data are stored, discussed, or processed
- Presence of any listening or surveillance devices in sensitive or secure areas
- Unauthorized storage of classified material
- Unauthorized access to classified or unclassified automated information systems
- Seeking access to sensitive information inconsistent with duty requirements
- Making statements expressing support of or sympathy for a terrorist group
- Making statements expressing preference for a foreign country over loyalty to the United States
- Expressing radical statements or actions threatening violence against a coworker, supervisor or others in the workplace

Information Transmittal

Report events or behaviors including, but not limited to:

- Unauthorized removal of classified or protected material from the work area without appropriate authorization
- Use of unclassified fax or computer to transmit classified material
- Improper removal of classification markings from documents
- Discussions involving classified information over a nonsecure telephone
- Concealment of foreign travel

Suspicious Behavior

Report behavior including, but not limited to:

- Attempts to expand access to classified information by repeatedly volunteering for assignments or duties beyond the normal scope of responsibilities
- Extensive use of copy, facsimile, or computer equipment to reproduce or transmit classified material that may exceed job requirements
- Repeated or un-required work outside of normal duty hours
- Unexplained or undue affluence
- Sudden reversal of financial situation or sudden repayment of large debts
- Attempts to entice DoD personnel into situations that could place them in a compromising position
- Attempts to place DoD personnel under obligation through special treatment, favors, gifts, money, or other means
- Short trips to foreign countries or travel within the United States to cities with foreign diplomatic activities for reasons that appear unusual or inconsistent with a person's interests or financial means
- Indications of terrorist activity

Derived from NISPOM Section 1-302 and DoDI 5240.6 Paragraph 6.2

Maintaining an Effective Program

Key Strategies

As an FSO, you are responsible for maintaining an effective CI program at your facility. Engaging in certain activities, on a regular basis, will help you do this effectively.

First, you must adhere to initial and annual training requirements. Ensuring employees receive security and CI training helps protect your facility and national security. But having an effective CI program involves more than just a yearly CI briefing. Another important activity is to establish a process for sharing security and CI best practices across all areas of the company, including personnel in CI, security, human resources, and information assurance, among other areas.

Once you establish and share CI and security best practices at your facility, you need to work to ensure facility employees apply these practices consistently throughout the organization.

Successful CI awareness and employee education are not one-time events; they are a continuous process. You should revisit these activities regularly and tweak them as circumstances require.

Review Activity

Which of the following activities can you use to promote CI awareness within your facility?

Select all that apply.

- ☐ Enlist your DSS CI Special Agent to brief employees
- ☐ Post CI-related material throughout the workspace
- ☐ Provide employees with CI training
- ☐ Share actual targeting examples with employees

Answer Key

Review Activity

Which of the following activities can you use to promote CI awareness within your facility?

- ☑ Enlist your DSS CI Special Agent to brief employees
- ☑ Post CI-related material throughout the workspace
- ☑ Provide employees with CI training
- ☑ Share actual targeting examples with employees

All of these are ways to promote CI awareness among your facility's employees.

Student Guide

Sensitizing Facility Employees to CI Concerns

Course Conclusion

Course Conclusion

Course Summary

In this course, you learned that in order for a CI program to be successful, a CI mindset needs to be ingrained into a facility's culture. Employee awareness is central to a successful CI program. As an FSO, your role is to help employees understand how they may be targeted and to encourage them to report all suspicious contacts, whenever they occur.

Lesson Review

Here is a list of the lessons in the course:

- Course Introduction
- Lesson 1: Identifying Employee Targets within Your Facility
- Lesson 2: Building a Culture of CI Awareness among Employees

Course Objectives

Congratulations. You have completed the Sensitizing Facility Employees to CI Concerns course.

You should now be able to perform all of the listed activities.

- Identify the key employee groups at your facility most likely to be targeted by an adversary attempting to gain information:
    - Identify the vulnerability of each of these groups
    - Identify the kinds of contacts these groups are likely to experience
- Identify ways to promote employee awareness and reporting of issues of CI concern