Thwarting the Enemy: Providing Counterintelligence and Threat Awareness to the Defense Industrial Base

Student Guide

October 2024

Center for Development of Security Excellence

Contents

Lesson 1: Course Introduction

Introduction

The Attack

> *[News Anchor] We are receiving reports of multiple explosions at the Jebel Abbas Air Base near Dubai. We have not yet confirmed the cause of the explosions. We do know that Jebel Abbas houses around five thousand U.S. servicemembers, as well as their spouses and children. We will keep you updated as additional details come in.*

Introduction

When you contract with the United States Government, lives are in your hands. The information you have available to you can put national security at risk, whether it is classified or not, and America's adversaries are already trying to contact you.

In 2022, cleared contractor personnel submitted more than 26,000 Suspicious Contact Reports, or SCRs, notifying the Defense Counterintelligence and Security Agency, or DCSA, that someone was trying to acquire access or information through them. That is an eight percent increase from 2021, and the numbers are expected to grow.

Every year, adversaries find ways to compromise national security, damage contracting companies, and exploit individuals like you. You must always remain vigilant. This air base and this attack are fictitious, but the risk is real. Take a moment to review the course objective.

- Analyze the given scenario(s) for indicators for targeted foreign collection and take appropriate action.

Your Investigation

In this course you will take a lead role investigating the fictional attack on Jebel Abbas. This will give you a detailed look at how America's adversaries can gain access to information and how contractors like you can protect themselves.

As you will soon see, this attack was the product of many separate incidents over a long period of time. Each step of the way, the Foreign Intelligence Entities, or FIEs, conducting this operation gained a little more information and a little more access, until they had what they needed to strike. You will not have to work alone. Through the course Resources, you have access to a library of useful materials, and throughout the course you will work with experts who can give you insight into different pieces of the investigation.

Facility Security Officer (FSO)

[FSO] Hello. I am excited to work with you. I am a Facility Security Officer for a cleared defense contractor. FSOs like me are responsible for the overall security at our facilities and for ensuring that security regulations and policies are followed. Every cleared contractor facility has an FSO, including yours. I will check in from time to time to let you know what facilities like yours need to watch out for.

Role: Facility Security Officer

Responsibilities:

- Managing the overall security of a contracted facility
- Ensuring security regulations and processes are followed

Counterintelligence Special Agent (CISA)

[CISA] Hi. I am a Counterintelligence Special Agent, or CISA, with DCSA. We are an agency within the Department of Defense. A large part of our role is to support cleared defense contractors like you. We also rely on you to be our eyes and ears within the defense industrial base. My role during this investigation, and others like it, is to provide input to the appropriate investigative agencies. I will also give you guidance and tell you more about what DCSA can do for you and how you can help DCSA.

Role: Counterintelligence Special Agent

Responsibilities:

- Provide counterintelligence support to cleared defense contractors
- Investigate and respond to potential instances of FIE targeting efforts and/or collection attempts
- Provide input to investigative agencies

Adversary

[Adversary] Your Department of Defense wants to call me an adversary, but I consider myself an artist. It takes a lot of creativity, and a lot of effort, to pull off something like Jebel Abbas. Yes, that was me. My art requires me to remain anonymous, and I am very good at that. You could pass me on the street, or sit in the cubicle next to mine, and not know who I am. As you look through the timeline of my work, you will see the techniques and tools at my disposal, and while you review what I have already done, I can start planning my next piece. Good luck.

Identity: Unknown

Location: Unknown

Responsibilities:

- Terrorism
- Espionage
- Cyber Operations
- Insider Recruitment

Lesson 2: Targeting at Conferences, Symposiums, and Trade Shows

Targeting

Lesson Introduction

> *[News Anchor] Details are still slow in coming, but the Department of Defense has confirmed that the attack on the Jebel Abbas Air Base involved a drone strike on the civilian areas of the base. The current toll stands at 15 dead and 44 injured. A Department of Defense spokesperson has announced that an investigation into the circumstances of the attack is now well underway.*

Your investigation is on the adversary's trail, learning what information they had access to and when. The earliest activities you can track were several months before the attack.

Targeted at Conference – Dr. Smith

Several months before the attack, Dr. Darius Smith, a cleared academic, attended an international conference. Dr. Smith is an expert in fuel cell technology for Unmanned Aerial Vehicles, or UAVs. In the weeks before the conference, Dr. Smith exchanged emails with another researcher with similar interests, who asked interesting and intellectually challenging questions. They made plans to meet up at the conference. Dr. Smith had several conversations with his new friend. He would never knowingly reveal sensitive or classified information, but through a series of seemingly innocent conversations, he shared many details. Although no one detail was classified, taken together, they painted a more complete picture. As it happens, his new friend was a representative from a foreign group trolling the trade show for information about UAV technology and experts to exploit. The pieces provided by Dr. Smith put them on the path to their ultimate goal.

Profile: Dr. Darius Smith

Occupation: Electrochemist

Specialty: Fuel Cells

Compromised:

- Efficient UAV fuel cells
- Specific components to obtain

- Possible industry experts to elicit

Facts:

- Smith was elicited weeks before the conference.
- Smith planned to meet contact during the event.
- Smith revealed several unclassified details.
    - Unclassified details can be combined to reveal classified information.
- Contact was member of a foreign organization collecting information.

Knowledge Check – 1

When discussing work details at a conference, what is the best attitude to take?

Select the best response; then check your answer in the Answer Key at the end of this Student Guide.

○ Sharing ideas with colleagues is a great way to learn. As long as classified or confidential details are not discussed, there's no harm.

○ Exchanging ideas with others in the same field is the best way to advance technology. Within the safe environment of an invitation-only conference, no topic should be off limits.

○ It is best to do more listening and less talking.

Targeting at Conferences, Symposiums, and Trade Shows

As a Federal contractor, it is always important to engage in active listening, especially when elicitation may be involved. One unclassified detail in isolation may not seem to pose much risk, but a clever adversary can combine many unclassified details together to reveal critically sensitive insights, whether classified or unclassified.

- Estimates indicate that as many as 1 in 20 attendees at conferences are there strictly to collect information. It is a common tactic, and for good reason.
- Conferences, conventions, and trade shows directly link programs and technologies with knowledgeable personnel.
- Technical experts may be invited to attend international events specifically to create opportunities to ask them about restricted, proprietary, and classified information.

- FIEs typically pose as other parties, including attendees, exhibitors, scientists, representatives of other nations, or even potential customers.

By subtly directing the conversation with questions and comments, they can collect enough details to piece together the bigger picture, as Dr. Smith learned too late.

Frequently, adversaries target specific types of information:

- DOD technical plans and budgets
- Proprietary formulas and processes
- Blueprints and prototypes
- Research findings
- Cleared and uncleared employee vulnerabilities
- Vendor and supply chain information
- Software information
- Company information

While you may already be cautious with technical information like plans and budgets, proprietary formulas, prototypes, and research findings, you must also protect information about employees, vendors, software, and other details about your company.

Key Indicators

> *[FSO] As an FSO, it is my job to make sure what happened to Dr. Smith does not also happen to you. I want to make sure you know what to watch for. Before the conference, Dr. Smith received an unsolicited email from an expert he had never met, and the conversation eventually turned to technical details.*

Before the event: As it happens, cleared contractor personnel and academics can be targeted weeks or even months before an event. Other similar techniques adversaries might use include:

- Offering an all-expenses-paid invitation to lecture in a foreign nation
- Requesting a summary of the requested presentation or brief months prior to the lecture date
- Attempting to visit the target facilities before the event
- Approaching or interacting with the target en route to the event

During the event: When you finally arrive, you cannot let down your guard. You will need to be on watch for indicators such as:

- Telephone monitoring and hotel room intrusions
- Conversations involving classified, sensitive, export-controlled, or dual use technologies or products
- Casual conversations during and after the event hinting at future contacts or relations
- Foreign attendees' business cards or nametags not matching their stated identities or affiliations

Knowledge Check – 2

How should Dr. Smith and his organization have prepared for this threat?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

□ Never participate in conferences and trade shows
□ Confront suspected FIEs and demand the truth
□ Request a detailed travel briefing prior to the conference
□ Specify as an organization what information can be shared and with whom

Countermeasures

> *[Adversary] Your organization cannot very well avoid all international events. And picking fights with suspected FIEs will not help you, either. If you really think you have spotted me, your best response is somewhere in between.*

- Be prepared well in advance.
- Request detailed travel briefings from DCSA CISA.
- Consider how to protect equipment and software.
  - Bring a sanitized laptop.
  - Bring mockup displays of products.
- Be mindful of what information is being shared, where, when, and to whom.

    - Restrict information you provide to what is necessary for travel and hotel accommodations.

Conclusion

The attack on Jebel Abbas started at a conference, with an adversary pulling enough details from an unwitting insider to uncover classified information about a key defense technology. If Dr. Smith had been less trusting and more vigilant, he could have set back the attackers' plans. This was only the first in several failures that led to the catastrophe.

Lesson 3: Insider Threat

Insiders and Elicitation

Lesson Introduction

> *[News Anchor] Our top story this morning, two more victims of the Jebel Abbas drone attack passed away during the night. This brings the death toll to 23, including five children under the age of 12. No one has yet taken responsibility for the attack on our military families, which is unusual and concerning for an event such as this. When asked this morning whether there was evidence the attackers had help from within the Department of Defense, a spokesperson for the White House declined to comment, stating the investigation is still in its early stages.*

Insider threat refers to the likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the national security of the United States. The attackers were assisted by several insiders as they planned and executed the attack.

The Unwitting Insider – J. Knowles

A few months after Dr. Smith’s encounter with the adversary at a conference, Jess Knowles, a cleared contractor who designs stealth systems, received an email that appeared to be from a student at her alma mater. The student stated she had heard about Ms. Knowles from one of her professors and was interested in doing the same type of work. She requested an opportunity to interview Ms. Knowles about the kinds of projects she worked on.

The student’s attempts at flattery made Ms. Knowles suspicious, and she deleted the email without replying to it, protecting herself from the adversary. However, she did not report the encounter to her FSO. If she had, her FSO and DCSA CISA could have taken steps to protect other insiders from similar elicitation attempts.

Profile: Jess Knowles

Occupation: Materials Engineer

Specialty: Stealth Systems

Facts:

- Knowles received an email from a student requesting an interview.

- Student’s attempts at flattery made Knowles suspicious.
- Knowles did not report the contact as required.

Knowledge Check – 1

Which of the following contacts would you consider reporting?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

☐ An ex-colleague asks detailed questions about work on ongoing classified projects.

☐ A potential international customer requests technical details for export-controlled products.

☐ A colleague regularly prods you for personal details about your financial situation.

☐ You receive an unsolicited email asking you to review a technical paper in your area of expertise.

Elicitation

An ex-colleague with detailed questions, a potential customer requesting technical data, a colleague showing unusual interest in sensitive projects, and an unsolicited request to review papers are all examples of elicitation that would need to be reported to your FSO.

Elicitation is a structured method of communication used to extract information from people without making them aware that they are a collection target. Elicitation can sound like common conversation, and that is what makes it so insidious. A skilled adversary rarely asks you for all your information at once. They will continually elicit small details from you over a period of time, piecing them together to form a larger picture.

Elicitation Tactics

Elicitation tactics work because people exhibit the same tendencies regardless of the context, allowing adversaries to exploit human nature and use it against you. Elicitation preys on specific human tendencies.

Tendency to complain

“I think you deserve more credit than your company gives you.”

When people feel negatively about something, they want to be heard. FIEs may influence people to complain and potentially reveal more than they mean to.

Questionnaires and surveys

"In your experience, what are the biggest challenges faced in developing heat-resistant materials for hypersonic vehicles?"

FIEs may try to legitimize the kinds of specific, invasive questions they want to ask. Experts are often asked to answer surveys from other experts, making the elicitation seem benign.

Feigning ignorance

"That is so interesting! How can the computer recognize what it sees through its sensors?"

FIEs may pretend not to know information about the subject, hoping to get their target talking and inadvertently reveal bits of sensitive information.

False testaments

"I just read an author who said our modern UAVs have become completely autonomous."

FIEs can prey on people's desire to correct false information, revealing sensitive details in the process.

Flattery

"I enjoy getting the chance to talk to people like you who are really pushing the industry forward."

FIEs can use simple flattery to build a rapport with their targets, encouraging them to let down their guard.

Quid pro quo

"The financial situation at our company is interesting, to say the least. I do not know whether you are open to sharing…"

FIEs can subtly hint or openly offer to share information, resources, or more in exchange for what you know.

Paper reviews

"One of our team is publishing a white paper on legal issues with civilian drones. Would you be willing to look it over?"

FIEs may ask experts to review seemingly irrelevant papers, either to gauge the target's access to sensitive information or to glean information from their comments.

Bracketing

"In one year, our competitors managed to increase their processing speed from 8 to 12 GHz using only eight cores. Are your machines at least comparable?"

Rather than ask for a specific number or figure outright, FIEs might provide a range of possible figures to elicit clues about where your information falls.

Oblique references

"We do not use those systems anymore, not with last year's big changes in radar resolution."

FIEs may make subtle or veiled references to classified information to gauge your reaction and how much you know.

Criticisms

"There are a lot of new companies in your market that are leaving yours behind. Do you really think you can keep up?"."

FIEs may criticize your or your company's work, hoping you may reveal sensitive details in your defense.

Elicitation Countermeasures

[CISA]:Deflecting suspected elicitation may make you feel awkward or uncomfortable in the moment—adversaries count on that reaction to keep you involved in the conversation. However, you respond, remember: Elicitation is a suspicious contact that must be reported to your FSO. If Ms. Knowles had reported her contact, it would have prevented more trouble for her office. If I suspect I am being elicited, there are several tactics I use to deflect the attempt. Select each countermeasure to learn more.

Change the topic

Elicitation: "I always thought your line of work was so interesting! What kind of projects have you worked on?"

Response: “They only give me the boring projects. For interesting problems, I enjoy gardening. I finally got my orchids going this year.”

When you suspect you are being elicited, the simplest thing to do is to move the conversation to a safer subject.

Take control of the conversation

Elicitation: “I can never stand working with the software developers, can you? I feel like they never understand our requirements.”

Response: “I never speak badly about the developers. We still need them to get things done. Production is a team effort. I feel a lot of people forget that.”

Closely related to changing the topic, taking control of the conversation puts you in the active role and lets you keep the topic on safer ground.

Deflect a question with a question

Elicitation: “I never quite understood. How does the product work without overheating?”

Response: “That gets pretty complicated. How long have you been in the business?”

Asking your own question can help you steer the conversation and put the elicitor in a position where they have to respond to you instead of vice versa.

“Why do you ask?”

Elicitation: “Does your company make its own motors, or do you source them externally?”

Response: “Those decisions are made outside my area. Why do you ask?”

When an elicitor asks specific questions, you can feign ignorance and ask about their interest in the subject. This can dissuade them from further elicitation attempts.

Refer them to public websites

Elicitation: “I would like to know more about other products your company makes.”

Response: “We have a lot of our catalog on our website, and our sales reps are very helpful.”

The public websites for your company or university can serve as important buffers against attempts to get information from you.

Provide only vague answers.

Elicitation: “How many can your facility make in a month? One thousand? Two thousand?”

Response: “That depends on how many orders we get.”

When an elicitor starts to push for specific details, keep the conversation on the vaguest terms.

Casually request a photo.

Elicitation: “Here is my card. I would love to explore a partnership with your company.”

Response: “Great! Do you mind if I take a picture with you? I always prefer to keep photos of important clients.”

If an elicitor is pushing to start a longer-term relationship, casually requesting a photo can put them on the defensive.

The Unwitting Insider – J. Stephenson

Two weeks after failing to elicit information from Ms. Knowles, the adversary tried again with one of her colleagues. Jake Stephenson was an engineer working on the materials and construction of UAVs. He also had a sports gambling habit that had put him several thousand dollars in debt, so when he received an unsolicited email offering compensation for him to review technical papers and provide insight and feedback, he was all too happy to agree. The work soon escalated to providing answers to difficult technical problems. He suspected it may not be legal but decided not to ask questions.

His colleagues failed to notice changes in his behavior at first. Stephenson had always been abrasive. As he continued working with the adversary, he communicated less and less with his team, and they wondered what might be going on in his personal life. When the paid assignments finally dried up, he surprised his coworkers by buying an expensive house in a new city and quit his job.

Profile: Jake Stephenson

Occupation: Materials Engineer

Specialty: Manufacturing

Facts:

- Gambling habit placed him in debt.
- Stephenson received payment to review technical papers and provide expertise.

- Stephenson ignored concerns the work was illegal.
- Stephenson's interactions with colleagues worsened.
- Stephenson displayed sudden, unexplained affluence.

Compromised:

- UAV component specifications
- UAV structural requirements and tolerances

Knowledge Check – 2

Jake Stephenson became an insider threat without being reported by his colleagues. How do you feel about reporting your coworkers' behavior or details of their personal life or lifestyle?

Select the best response; then check your answer in the Answer Key at the end of this Student Guide.

○ Work is work. My coworkers' personal lives are none of my business.

○ Unless I can provide a specific work-related example, reporting anything would be unprofessional.

○ It might make me uncomfortable, but I would report my concerns.

Indicators of Insider Threats

[Adversary] Even though personnel are required to monitor their colleagues' behaviors, Americans can feel so awkward about it. I rely on that awkwardness to do my job successfully. If you were to watch closely, you would start to notice patterns of vulnerability in some insiders. Sometimes these are patterns I follow when I look for a useful target. Other times these are signs I have already co-opted them.

Each member of the workforce has the responsibility to monitor their colleagues' behavior. Insider threats often show similar patterns:

- Misuse of alcohol/substances
- Mental health issues
- Extreme interpersonal difficulties
- Hostile or malicious behavior
- Criminal behavior

- Divided loyalty or allegiance
- Financial issues
- Unexplained or sudden affluence
- Unreported foreign contact or travel
- Inappropriate interest in classified info
- Misuse of information systems
- Working hours inconsistent with role
- Repeated security violations
- Reluctance to take a polygraph

You should report all these behaviors.

Countermeasures

Your organization is required to have plans in place for dealing with insider threats. You can also view the course resources for additional information on countermeasures.

Plans will include the following countermeasures at minimum.

Insider threat training

Your organization is required to provide training on the risks of Insider Theat, and the Center for Development of Security Excellence (CDSE) provides a library of awareness materials. Take all training available and pay close attention.

Briefings on elicitation

Attend briefings on elicitation methods and countermeasures. Elicitation can come from insiders as well as outsiders.

Be alert to other employees

Be alert to the actions of other employees and report when necessary. You might think that someone else will report concerning behaviors and relieve you of the responsibility. Stephenson’s colleagues might have thought the same thing. If any of them had reported his interpersonal difficulties and sudden affluence, DCSA could have stepped in to limit the damage.

Monitor foreign visitors

Be sure to monitor the activities of foreign visitors for indicators they are targeting personnel or technology.

Restrict sensitive information

Limit the dissemination of sensitive information based on whether that person has a need to know.

Monitor information systems

If you use information systems to house classified information, you must have a plan in place to monitor them for reportable anomalies.

Conclusion

The knowledge and skills personnel like you bring can help the United States to maintain its technological advantage over its adversaries. If Ms. Knowles had properly reported her encounter with the adversary, and if Stephenson's colleagues had reported his behavior, crucial information would have been secure. Your investigation is not over yet. Continue on to uncover more evidence of the adversary's scheme.

Lesson 4: Unsolicited and Direct Request

Unsolicited and Direct Requests

Lesson Introduction

> *[News Anchor] We are receiving word this morning that the first arrest has been made in connection with the attack on the Jebel Abbas Air Base. Jake Stephenson, a former defense contractor, was detained at Hartsfield-Jackson Airport in Atlanta, Georgia. It is not clear at this time what role Mr. Stephenson played in the attack or whether he was attempting to flee law enforcement. A spokesperson for the Department of Defense declined to comment on the ongoing investigation.*

The security failures you have looked at so far have all had one thing in common: The adversary made unsolicited contact with insiders. There are many ways FIEs can use unsolicited and direct requests to manipulate insiders into providing information. The people planning the attack on Jebel Abbas made good use of the technique.

The Social Media Contact – C. Li

Crystal Li was a specialist in satellite communication, using her expertise to enable UAV operators to reach targets worldwide. She knew her skills were in high demand, so when she received a message from a recruiter on a professional social media site, asking her to apply to a highly compensated corporate position, she was excited for the opportunity. The application process was intensive, requiring her to explain how she would work with colleagues on various realistic scenarios. She was disappointed when she never heard back regarding her application, but eventually she simply moved on.

Profile: Crystal Li

Occupation: Communications Engineer

Specialty: Satellite Operations

Facts:

- Li received an invitation from a recruiter to apply to a well-paid position.
- The application process required detailed information.
- Li never heard back regarding the position.

Compromised

- Solutions to issues in satellite communication
- Names of colleagues and supervisors

Knowledge Check – 1

What is your attitude when someone asks you for information on social media?

Select the best response; then check your answer in the Answer Key at the end of this Student Guide.

○ I am always suspicious of messages on social media, even if it is from someone I know.

○ As long as the person has a good reason, there is no harm in sharing unclassified information.

○ I only respond to the request if I know who the person is.

Unsolicited and Direct Requests

FIEs frequently collect intelligence through seemingly normal social or professional contacts. These contacts could come in the form of:

- Job applications and resumes
- Requests for information about products
- Messages on social media

Anyone can be a target. Even if you do not think you have access to information adversaries would want, you could be targeted simply to get access to other targets. Unsolicited and direct requests are so common because they can be so effective. FIEs use unsolicited messages to prey on basic human tendencies, including the:

- Desire to be polite and helpful
- Desire to appear well informed
- Desire to show off
- Desire to correct others’ comments
- Tendency to underestimate the value of the information you give
- Belief that others are fundamentally honest

Social Networking Services (SNS)

About five billion people, more than half the world's population, use social media. As the world becomes more connected by Social Networking Services, or SNS, the potential for these sites to be used by adversaries also increases.

Adversaries can use information posted to SNS, including work, location, and travel information, to collect data for their operations. They can use SNS messaging capabilities to make direct contact with cleared contractors and academics, carefully crafting a user profile for their purposes. They can even spread *misinformation* to influence people and events. You should never trust the contacts, information, or links you find on social networks.

Knowledge Check – 2

Which of these unsolicited contacts should be reported?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

- □ A long-time customer emails with concerns about their most recent order, and you confirm their identity.
- □ A faculty member at an overseas university emails suggesting a long-term research partnership.
- □ A well-known tech company sends an email offering a $1000 gift card.
- □ You receive an urgent phone call from the U.S. Treasury demanding company financial records, or they will take legal action against you.

Recognizing Suspicious Requests

> *[Adversary] How did you do with that question? If you take the time to confirm your customer's identity, you are typically safe. The potential research partner? I often pose as a potential research partner. You would want to take real time to verify my identity there. The link you can click to get a free thousand dollars is definitely from me. Clicking that will put a virus on your computer. And you would be amazed how many people fall for the give-me-your-records-or-get-arrested scam.*

Indicators or Suspicious Messages

How do you recognize whether a message you receive is legitimate? Your first reaction to unsolicited messages should always be suspicion. These indicators can help to confirm that a message is an adversary’s attempt at contact. Here is an example of an adversary’s unsolicited contact attempt.

Message
From: alazarevski@vstat.mk To whom it may concern, I am a technical consultant for a corporation doing work on behalf a foreign defense ministry. My client is interested in your company’s xROD cybersecurity suite. We have inquired about similar systems from other vendors, but as yet they have not worked with us regarding export controls. To be clear, export controls will not be an issue. Nevertheless, if this is impossible for other security concerns, please disregard this email. Regards, Alexei Lazarevski

Foreign address

From: alazarevski@vstat.mk

The requester sends the request using a foreign address.

Unknown sender

“Regards, Alexei Lazarevski”

The requester is someone the recipient has never met.

Student / consultant

“I am a technical consultant…”

The requester identifies themselves as a student or consultant.

Foreign government

“…on behalf of a foreign defense ministry.”

The requester identifies their employer as a foreign government or states the work is being done on behalf of a foreign government or program.

Specific programs

“…your company’s xROD cybersecurity suite.”

The requester asks about technology related to a defense program, project, or contract, and uses acronyms specific to the program.

Sensitive request

"…they have not worked with us regarding export controls."

The requester insinuates the third party they work for is "classified" or otherwise sensitive, or admits they could not get the information elsewhere because it was classified or controlled.

Security and export licenses

"…export controls will not be an issue."

The requester advises you not to worry about security concerns or export licenses.

Note to disregard

"…please disregard this email."

The requester advises the recipient to disregard the request if it causes a security problem, or the request is for information you cannot provide due to security classification or export controls.

Countermeasures

> *[FSO] As an FSO, I am often asked how to keep from being taken advantage of by direct messages. I always tell my colleagues to start by viewing unsolicited and direct requests with suspicion, especially ones you receive via the internet. Only respond to people if you can confirm their identity and address. If you cannot confirm their identity, do not respond in any way. Instead, report the incident to your FSO.*

Conclusion

By now you should see the pattern. Time and again, the adversary was able to make progress on their plan through the use of unsolicited and direct messages. Through Ms. Li, they were able to get details about technical issues that they could not solve themselves and access to other experts. After these initial stages, the plan became more ambitious. Continue on in your investigation to see how they were able to put the pieces together.

Lesson 5: Suspicious Network Activity

Suspicious Network Activity

Lesson Introduction

> *[News Anchor] We begin this evening with a potential connection between the Jebel Abbas Air Base attack and a cyberattack on AES, a company contracting with the Federal government to produce advanced UAVs. The event took place in March and was still being investigated by the Department of Defense when Jebel Abbas was attacked.*

The internet has provided our adversaries with powerful tools that their twentieth-century counterparts could only have dreamed of. Using only a little code and a little manipulation, the people responsible for the Jebel Abbas attack were able to access key data for UAV parts and materials.

The Big Phish – E. Arbor

Eleanor Arbor was a supply chain coordinator for a cleared contractor. Her role required her to have detailed information about different parts and systems UAVs used. This made her a prime scamming target. She received an email that appeared to be from one of their vendors about urgent changes to their delivery schedules and an attachment with more information. In her rush to handle the situation, Ms. Arbor failed to notice key details that could have tipped her off that the email was not genuine. In only a moment, her computer was infected with malware that began siphoning information to a server outside the United States. By the time her company was able to stop the leak, key information about the company and the construction of the UAVs had already been lost.

Profile: Eleanor Arbor

Occupation: Supply Chain Manager

Facts:

- Arbor received an urgent email with an attachment.
- In her sense of urgency, she overlooked indicators.
- The attachment contained a virus that siphoned away information.

Compromised

- Part numbers and suppliers

- Budget and financial information
- Personnel files

Knowledge Check

How should your facility handle suspicious network activity like this?

Select the best response; then check your answer in the Answer Key at the end of this Student Guide.

○ As far as I know, network activity is not routinely monitored. System administrators are busy enough as it is.

○ Suspicious network activity is dealt with internally. If it involves an employee, that person is subject to reprimand.

○ Suspicious network activity is a serious concern, and there are specific procedures in place, including reporting activity to the authorities, if warranted.

Suspicious Network Activity

Your office must have detailed security plans in place for your computers and networks. Consider: As our world becomes ever more interconnected, the risk of cyberattacks grows alongside it. Anyone with access to computer systems, sensitive information, or cleared personnel can be a target. The goal is not always to steal information. Sometimes adversaries want to destroy information or hold it for ransom. Sometimes they are after people, trying to find potential insiders to exploit or co-opt. FIEs have many tools at their disposal, including:

- Hacking directly into systems
- Using malware and trojan viruses to gain access to systems and information
- Directly communicating with or eliciting insiders via email or social media platforms
- Inputting falsified or corrupt data onto systems

Indicators of Suspicious Network Activity

[CISA] In my work as a CISA, I see a lot of cases where FIEs and insiders attempt to gain access to controlled or classified information on their networks. Depending on the tools they use to execute these attacks, many of the indicators of these attempts are visible on individual computers or networks. These include unauthorized system access attempts, unauthorized system access to, or disclosure of, information, any acts that interrupt or result in a denial of service,

unauthorized data storage or transmission, and unauthorized hardware and software modifications.

Indicators on Computers and Networks

- System access attempts
- Disclosure of information
- Denial of service
- Data storage or transmission
- Hardware or software modifications

As we learned from Ms. Arbor, system defenses against unauthorized access are important, but they are not enough. It's the responsibility of all personnel to be on guard against intrusions. Be skeptical of any email or message you receive from unknown senders. Even if the sender seems familiar, pay close attention to the email address and take action to verify their identity. Do not click any links or attachments in these messages until you have confirmed the identity of the sender. To stay up to date on trends and risks in cybersecurity, be sure to review the Targeting U.S. Technologies report in this course's resources, which summarizes the types of threats that have been reported, where they come from, and what they target.

Indicators in Personal Contacts

- Unknown senders
- Suspicious addresses
- Suspicious links or attachments

Verify the identity of known senders before responding.

Countermeasures

As with all risks, it is vital to focus on prevention against cyberattacks. The best time to act is before an attack takes place.

- Conduct computer audits to monitor for suspicious activity, at least weekly, ideally daily.
- If you detect any intrusion attempts, report them immediately.
- Good firewalls are important, but do not rely on them to protect against all attacks. Many of the best defenses are behaviors, not technology.

- Avoid responding to any unknown requests for information. These requests must be reported.
- In the event of a severe cyberattack, disconnect your computer systems temporarily to limit the damage.

Your policy and procedures for protecting classified or sensitive information may be described in your company's Technology Control Plan, or TCP.

Technology control plans

A TCP is often required by the National Industrial Security Program Operating Manual, or NISPOM, and International Traffic in Arms Regulations, or ITAR. It describes how your company controls access to its export-controlled technology, keeping American data within American borders. It outlines the specific information that has been authorized for release and to whom. By following the requirements of your TCP, you can protect classified and export-controlled information, as well as control access to information by foreign visitors and foreign-born employees.

Conclusion

Ms. Arbor was the target of a simple act of manipulation. What appeared to be an urgent message from a vendor turned out to be a sophisticated attack on her company, one that put the adversary several steps closer to a devastating attack on U.S. armed forces and their families. Continue your investigation, where you will see what happened when the adversary and their target came face to face.

Lesson 6: Foreign Visits

Foreign Visits

Lesson Introduction

> *[News Anchor] Dominoes continue to fall in the ongoing investigation into the Jebel Abbas attack. Dynamic Avionics, a subcontractor assisting in the manufacture of UAVs, is being formally sanctioned by the Federal government for its failure to protect classified information. Experts indicate this could include tens of millions of dollars in fines.*

You have looked at ways adversaries can exploit your access remotely. They can also exploit direct access to your facilities. It is crucial to have policies and practices in place to keep your facilities secure.

The Foreign Visit – E. Benedetto

Ed Benedetto was a manager at a facility producing parts for advanced UAVs, as well as other defense-related products. He was part of a group hosting a visit from a long-time customer from a West Asian nation wanting to manufacture traditional aircraft. The morning of the visit, Mr. Benedetto was surprised when one of the visitors had been replaced by a different representative. She apologized for the last-minute change and explained that her predecessor had to retire for medical reasons. The tour continued as planned.

The new representative asked several sophisticated questions about the manufacturing processes and equipment involved. Mr. Benedetto answered her questions. He did not directly reveal any classified information, but in his effort to be polite, he revealed many small details. The adversary was able to leave the facility with vital data about how to use the equipment and materials to manufacture UAVs.

Profile: Ed Benedetto

Occupation: Manufacturing Manager

Facts:

- Hosted foreign visit from customer.
- One representative replaced last-minute.
- Representative asked detailed questions.
- Many unclassified details combined to reveal classified information.

Compromised

- Manufacturing equipment and methods
- Facility logistics

Knowledge Check

How could the subcontractor have better prepared for the foreign visit?

Select the best response; then check your answer in the Answer Key at the end of this Student Guide.

○ The subcontractor should have made more detailed contingency plans for these kinds of situations.

○ The subcontractor should have contacted DCSA about the visit to obtain the proper briefing and procedures.

○ Being successful in business requires trust in clients. There wasn't anything more they could have done in this situation.

Indicators of Foreign Visit Exploitation

> *[CISA] I will be blunt: Mr. Benedetto and his office should have contacted DCSA. It may be difficult to imagine that FIEs could persuade you to give them access to your facilities, but any CISA can tell you it happens. Threats can come from long-term visitors, such as exchange employees, official government representatives, or students; frequent visitors, like sales representatives and business associates; or one-time visitors.*

In general, be on the lookout for these indicators:

- Requests for information outside the scope of what was approved for discussion
- Any attempts by attendees to contact you before, during, or after the visit
- Any signs of hidden agendas associated with the stated purpose of the visit
- Visitors or students requesting information and becoming irate upon denial
- Individuals bringing cameras where no photographs are allowed
- Any last-minute changes to the visitor list

Countermeasures

So how could Mr. Benedetto and his organization have better prepared for the visit? It is vital to contact DCSA before an event takes place, so you can get specific guidance for protecting your facility.

1. DCSA will provide briefings for procedures you can use during the visit.

2. Before the visit, walk the route you will take and watch for potential vulnerabilities. Are there places where a visitor could drift away from the group or see sensitive information or equipment?

3. Make sure everyone participating in the visit has a common understanding of the restrictions you will place on the information. Remember, your organization should have a Technology Control Plan with much of this information.

4. During the visit, ensure visitors do not bring any kinds of recording devices with them, including cell phones.

5. After the visit, have the team participate in a debrief and discuss everything that occurred. Give people an opportunity to bring up any potential concerns that would need to be reported.

Conclusion

Foreign visits can be important opportunities to connect with customers, business partners, and experts. An adversary's visit to your facility is a terrible time to be careless or ill prepared. Work closely with DCSA and plan the visit in detail to prevent serious consequences. Continue on in your investigation.

Lesson 7: Solicitation and Joint Venture

Joint Ventures

Lesson Introduction

> *[News Anchor] We are still anticipating the report of the investigation into the Jebel Abbas attack later this week. In advance of that release, the Treasury Department has announced sanctions on the al-Sultan Technical Institute in Muscat, Oman. It is not yet clear what role the institute played in the attack.*

Businesses and universities operating joint ventures with international institutions must go to great lengths to protect their information.

The Joint Venture – D. Henson

Dee Henson was an engineer at a facility producing UAVs. She was ambitious and excited to further her career in the industry, so when her company began hosting engineering internships in partnership with domestic and international universities, she offered to be a mentor. One of her interns was a student from Oman. Eager to impress her student, she let slip key details about the manufacturing process that the student did not need to know. She never suspected that, after each conversation, he took detailed notes, which he scanned and sent to his handler overseas via an encrypted mobile chat application.

Profile: Dee Henson

Occupation: Electrical Engineer

Specialty: UAV Circuitry

Facts:

- Mentored domestic and international students.
- Revealed key details to international student.
- Student transcribed notes and sent them home.

Compromised: Signal processor integrations

Knowledge Check

When a facility enters into a joint venture, what types of protection measures, if any, should be put into place?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

- ☐ If the defense contractor trusts who they've hired, there shouldn't be a need to put additional procedures into place.
- ☐ All documents being transmitted should be reviewed and translated, if necessary.
- ☐ The minimum amount of information should be shared, and it should be limited to what is necessary for the scope of the project.
- ☐ Foreign representatives should be given standalone computers and have limited network access.

Solicitation and Joint Venture

> *[Adversary] While joint ventures provide unique opportunities for business and academic institutions, they also provide me equally valuable opportunities. Ms. Henson's office should have paid attention to the information and access their interns had. Research partnerships, internship programs, and other services are great targets. They can get me and my colleagues inside American facilities to collect all the information we can get. They give me access to anyone on site with a security clearance and provide opportunities to build relationships with insiders I can exploit. Partnerships do all of this while giving me an appearance of legitimacy, helping me to evade suspicion.*

Indicators of Exploiting Joint Ventures

How could you spot a partner exploiting their access? Adversaries may attempt to mail or fax documents written in a foreign language to a foreign embassy or country to avoid detection. It is important to pay close attention to any information that venture partners transmit. Foreign visitors may also request increased or unrestricted access to Local Area Networks, or LANs, facilities, and company personnel information.

Countermeasures

We at DCSA often advise organizations like yours how to avoid being taken advantage of. These countermeasures are key.

- Review all documents being sent out or stored in the cloud, with a translator if necessary.
- Provide foreign representatives with standalone computers.
- Share the minimum amount of information appropriate to the scope of the venture or research.
- Be aware of the project scope and how to handle and report elicitation.
- Attend sustainment training to maintain your awareness of classification guidelines and security procedures.
- Refuse to accept unnecessary foreign representatives into the facility.
- Always comply with your company's Technology Control Plan, or TCP, including the use of badging systems and credentials.

Conclusion

Exploiting this internship program was the last step in the adversary's plan to construct their own UAV that could evade American defenses and attack a military installation. Any extended relationship with foreign workers, students, or academics must be carefully controlled and monitored for any signs of exploitation. The damage that could be done by adversaries acquiring information and recruiting insiders is too grave to ignore. Continue on to complete your investigation and to learn more about your responsibilities as a contracted employee to remain vigilant and report any suspicious activity you may find.

Lesson 8: Reporting Requirements

Reporting Requirements

Lesson Introduction

> *[News Anchor] For those of you who are just tuning in, another federal contractor has been arrested in connection with the attack on Jebel Abbas. Anara Shirvani, an aerospace engineer, has been arrested on conspiracy and terrorism charges. She joins Jake Stephenson as the second American arrested in the plot. Shirvani seems to have been a significant part of the conspiracy, and investigators are still looking into how her role went unnoticed.*

All personnel with access to classified information have a responsibility to report any indicators of potential threats to the security of the United States. Failure to report suspicious contacts or behaviors can lead to real consequences, not only for you, but for your organization and national security.

The Non-Reporter – C. Ruiz

Carlos Ruiz was a network engineer working for a cleared contractor. He had just joined the organization and was not in any way involved in the Unmanned Aerial Vehicle, or UAV, projects. After his first few weeks, he was curious about his colleagues and started searching for them on social media. There he found that one of his new colleagues, Anara, occasionally made posts that were sympathetic to violent separatist groups in the Middle East. Carlos was hesitant to report Anara. He did not want to cause trouble over nothing and was afraid of damaging his reputation at his new job. Ultimately, he decided to keep to himself. In spite of the fact that these posts fall under the DOD's reporting guidelines.

Profile: Carlos Ruiz

Occupation: Network Engineer

Facts:

- Searched colleagues on social media.
- Found colleague sympathizing with separatist groups.
- Failed to report.

DOD reporting requirements

The DOD's reporting and adjudicative guidelines, contained in SEAD 3 and SEAD 4, respectively, describe the kinds of behaviors that disqualify an individual from having access to classified information. Anara's posts fall under the guidelines in SEAD 3, Section F, and SEAD 4, Adjudicative Guideline C: Foreign Preference.

Knowledge Check

Consider the following behaviors. Which would you consider important enough to report?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

□ A colleague admits to you in private that they have excessive medical debt they cannot pay.

□ A colleague frequently offers to help and insists on working on projects outside their normal scope.

□ A colleague makes jokes about violence against women.

□ A colleague regularly comes to work appearing intoxicated.

Reporting Requirements

Medical debt, extra work, violent jokes, drug use: All of these are reportable behaviors. Under the NISPOM rule, all personnel are required to report:

- Indicators of insider threat
- Any potential risk to classified information
- Any potential loss or compromise of classified information.

If you see any of the indicators depicted in this course, follow your organization's reporting procedures and contact your FSO. Federal agencies do maintain hotlines for anonymous reporting if necessary, but your established reporting channels should be your first resort. These lists are not exhaustive. When in doubt, contact your FSO.

Recruitment behaviors

Contact your FSO if you or a colleague:

- Has contact with someone associated with a foreign intelligence, security, or terrorist organization

- Receives an offer of financial assistance by a foreign national other than close family
- Receives a request for classified or unclassified information outside official channels
- Engages in illegal activity or is asked to do so

Information collection

Contact your FSO if a colleague:

- Requests classified or protected information without authorization
- Requests witness signatures for destruction of classified information when you did not witness it
- If a colleague uses unauthorized cameras, recording devices, computers, or modems in areas where classified data are stored, discussed, or processed,
- If you find any listening or surveillance devices in sensitive or secure areas.

Contact your FSO if a colleague:

- Improperly stores classified material
- Gains unauthorized access to classified or unclassified automated information systems
- Seeks access to sensitive information inconsistent with duty requirements
- If a colleague makes statements expressing support or sympathy for a terrorist group, expressing preference for a foreign country over loyalty to the U.S, or threatening violence against a coworker, supervisor, or others in the workplace.

Information transmittal

Contact your FSO if a colleague:

- Removes classified or protected material from the work area without appropriate authorization
- Transmits classified material via unsecured means
- Improperly removes classification markings from documents

- Discusses classified information over a nonsecure telephone
- Conceals foreign travel

Suspicious behaviors

Contact your FSO if a colleague:

- Attempts to expand access to classified information by repeatedly volunteering for assignments or duties beyond their normal scope of responsibilities
- Extensively uses copiers, facsimiles, or computer equipment to reproduce or transmit classified material beyond their job requirements
- Frequently works outside normal duty hours when not required
- Demonstrates unexplained or undue affluence
- Suddenly reverses a financial situation or repays large debts
- Takes short trips to foreign countries or U.S. cities with foreign diplomatic activities for reasons that appear unusual or inconsistent with the person's interests and means
- Shows any indicators of terrorist activity

Conclusion

Carlos had an opportunity to report an insider threat at his company, and he did not take it. This was the last opportunity someone had to uncover the attack on Jebel Abbas before it took place. As a consequence, 23 people were killed, and Carlos will deal with the legal consequences of his inaction for years. Now that you have concluded your investigation, you can see how the attack resulted from a series of security failures. Continue to the next lesson to review what you have learned.

Lesson 9: Course Conclusion

Conclusion

Course Conclusion

> *[News Anchor] We are back in the studio now after the Department of Defense, or DOD, announced the release of their report into the attack on Jebel Abbas. Anara Shirvani, who was arrested on Monday, coordinated the conspiracy in the defense industrial base, connecting foreign operatives with American insiders and providing key intelligence overseas. The full extent of the damage and the cost of the lost information may never be fully known. The spokesperson also announced reprisals on the clandestine network. Arrests have been made in Oman and the United Arab Emirates, and plans are being made to extradite the conspirators to the United States.*

In this course, you saw how a series of security failures added up to allow a fatal attack on the United States. This scenario was fictional, but the risk is real.

You should now be able to recognize the six most common tactics FIEs use to gain access to American technology and information. As you have seen, many of these can be combined in insidious ways to take advantage of unwitting insiders, or to elicit and exploit witting insiders. You should also know what events or behaviors need to be reported to your FSO, whether someone is attempting to elicit information from you, or you have concerns about another insider in your organization. Remember, regardless of your position or your access, you are a target for America's adversaries. You must remain vigilant and you must report.

Course Review

Here is a list of lessons in the course:

- Lesson 1: Course Introduction
- Lesson 2: Targeting at Conferences, Symposiums, and Trade Shows
- Lesson 3: Insider Threat
- Lesson 4: Unsolicited and Direct Request
- Lesson 5: Suspicious Network Activity
- Lesson 6: Foreign Visits
- Lesson 7: Solicitation and Joint Venture

- Lesson 8: Reporting Requirements
- Lesson 9: Course Conclusion

Lesson Summary

Congratulations. You have completed the Thwarting the Enemy course.

You should now be able to analyze a given scenario for indicators of a foreign collection attempt to take appropriate action.

To receive course credit, you must take the Thwarting the Enemy examination. If you accessed the course through the Security Training, Education, and Professionalization Portal (STEPP), please use that system to access the online exam.

Appendix A: Answer Key

Lesson 2 Review Activities

Knowledge Check – 1

When discussing work details at a conference, what is the best attitude to take?

○ Sharing ideas with colleagues is a great way to learn. As long as classified or confidential details are not discussed, there's no harm.

○ Exchanging ideas with others in the same field is the best way to advance technology. Within the safe environment of an invitation-only conference, no topic should be off limits.

⦿ It is best to do more listening and less talking.

Points (0 for incorrect and 1 for correct): __________

Knowledge Check – 2

How should Dr. Smith and his organization have prepared for this threat?

□ Never participate in conferences and trade shows

□ Confront suspected FIEs and demand the truth

☑ Request a detailed travel briefing prior to the conference

☑ Specify as an organization what information can be shared and with whom

Points (0 for incorrect and 1 for correct): __________

Lesson 3 Review Activities

Knowledge Check – 1

Which of the following contacts would you consider reporting?

☑ An ex-colleague asks detailed questions about work on ongoing classified projects.

☑ A potential international customer requests technical details for export-controlled products.

☑ A colleague regularly prods you for personal details about coworkers on other projects.

☑ You receive an unsolicited email asking you to review a technical paper in your area of expertise.

Points (0 for incorrect and 1 for correct): __________

Knowledge Check – 2

Jake Stephenson became an insider threat without being reported by his colleagues. How do you feel about reporting your coworkers' behavior or details of their personal life or lifestyle?

○ Work is work. My coworkers' personal lives are none of my business.

○ Unless I can provide a specific work-related example, reporting anything would be unprofessional.

◉ It might make me uncomfortable, but I would report my concerns.

Points (0 for incorrect and 1 for correct): __________

Lesson 4 Review Activities

Knowledge Check – 1

What is your attitude when someone asks you for information on social media?

◉ I am always suspicious of messages on social media, even if it is from someone I know.

○ As long as the person has a good reason, there is no harm in sharing unclassified information.

○ I only respond to the request if I know who the person is.

Points (0 for incorrect and 1 for correct): __________

Knowledge Check – 2

Which of these unsolicited contacts should be reported?

☐ A long-time customer emails with concerns about their most recent order, and you confirm their identity.

☑ A faculty member at an overseas university emails suggesting a long-term research partnership.

☑ A well-known tech company sends an email offering a $1000 gift card.

☑ You receive an urgent phone call from the U.S. Treasury demanding company financial records, or they will take legal action against you.

Points (0 for incorrect and 1 for correct): __________

Lesson 5 Review Activities

Knowledge Check

How should your facility handle suspicious network activity like this?

○ As far as I know, network activity is not routinely monitored. System administrators are busy enough as it is.

○ Suspicious network activity is dealt with internally. If it involves an employee, that person is subject to reprimand.

◉ Suspicious network activity is a serious concern, and there are specific procedures in place, including reporting activity to the authorities, if warranted.

Points (0 for incorrect and 1 for correct): __________

Lesson 6 Review Activities

Knowledge Check

How could the subcontractor have better prepared for the foreign visit?

○ The subcontractor should have made more detailed contingency plans for these kinds of situations.

◉ The subcontractor should have contacted DCSA about the visit to obtain the proper briefing and procedures.

○ Being successful in business requires trust in clients. There wasn't anything more they could have done in this situation.

Points (0 for incorrect and 1 for correct): __________

Lesson 7 Review Activities

Knowledge Check

When a facility enters into a joint venture, what types of protection measures, if any, should be put into place?

□ If the defense contractor trusts who they've hired, there shouldn't be a need to put additional procedures into place.

☑ All documents being transmitted should be reviewed and translated, if necessary.

☑ The minimum amount of information should be shared, and it should be limited to what is necessary for the scope of the project.

☑ Foreign representatives should be given standalone computers and have limited network access.

Points (0 for incorrect and 1 for correct): __________

Lesson 8 Review Activities

Knowledge Check

Consider the following behaviors. Which would you consider important enough to report?

☑ A colleague admits to you in private that they have excessive medical debt they cannot pay.

☑ A colleague frequently offers to help and insists on working on projects outside their normal scope.

☑ A colleague makes jokes about violence against women.

☑ A colleague regularly comes to work appearing intoxicated.

Points (0 for incorrect and 1 for correct): __________

Total Points: __________