Student Guide

Insider Threat Awareness

Course Introduction

Introduction

Screen 1 of 2

Narrator: Welcome to the Insider Threat Awareness course. Benjamin Bishop, Gregory Allen Justice, and John Robert Neumann…what did each of these insiders have in common? Their coworkers saw them act suspiciously, and some suspected something was amiss. Yet, almost without exception, those coworkers said little about their suspicions. Coworkers have the best insight into changes in behavior and attitude among their colleagues. You are your organization's first line of defense against someone who could do harm to the workforce, information, and environment.

Screen text: Benjamin Bishop, Gregory Allen Justice, and John Robert Neumann…what did each of these insiders have in common? Their coworkers saw them act suspiciously, and some suspected something was amiss. Yet, almost without exception, those coworkers said little about their suspicions. Coworkers have the best insight into changes in behavior and attitude among their colleagues. You are your organization's first line of defense against someone who could do harm to the workforce, information, and environment.

This course is intended to help familiarize you with the subject of insider threat and provide guidance on what to do if you suspect that something is not right. Your coworkers and your organization are depending on you.

If you see or hear something, say something.

Learning Objectives

Screen 2 of 2

Narration: This course is intended to help familiarize you with the subject of insider threat and provide guidance on what to do if you suspect that something is not right. Your coworkers and your organization are depending on you.

Please review the course learning objectives.

Screen text: Learning Objectives:
After completing the Insider Threat Awareness course, you will be able to:

- Define insiders and insider threat categories
- Identify insider threat potential vulnerabilities and behavioral indicators
- Describe what adversaries want to know and the techniques they use to get information from you
- Describe the impact of technological advancements on insider threat
- Recognize insider threat, counterintelligence, and security reporting recommendations

Lesson 1
Insider Threat Categories

Learning Objectives
Screen 1 of 28

Narration: In this lesson, you will learn about the definition of insiders, insider threat, and its categories.

Screen text: Lesson 01 | Introduction

In this lesson, you will learn about the definition of insiders, insider threat, and its categories.

Learning Objectives

After completing this lesson, you will be able to:

- Define insiders and insider threat
- Describe insider threat categories

Insider Threat
Screen 2 of 28

Narration: It's very rare that an individual wakes up with the intention of betraying their company, harming their colleagues, or compromising national security. Research has consistently shown that malicious acts by insiders are seldom impulsive. That means that something happens over time that contributes to a trusted insider evolving into a malicious one. Usually it is some sort of perceived life crisis that the individual views as untenable. Eventually, if not dealt with in a healthy and adaptive manner, these stressors could influence a person to commit espionage, leak information, engage in targeted violence, or contemplate self-harm.

Screen text: Insider Treat

It is very rare that an individual wakes up with the intention of betraying their company, harming their colleagues, or compromising national security. Research has consistently shown that malicious acts by insiders are seldom impulsive.

That means that something happens over time that contributes to a trusted insider evolving into a malicious one. Usually it is some sort of perceived life crisis that the individual views as untenable.

Eventually, if not dealt with in a healthy and adaptive manner, these stressors could influence a person to commit espionage, leak information, engage in targeted violence, or contemplate self-harm.

Human Factors

Screen 3 of 28

Narration: Even though members of our workforce have been determined to be trustworthy custodians of classified or proprietary information, this does not make them immune to the human condition. Life happens, and we all have to deal with challenges, crises, and the obstacles that life will inevitably present.

Screen text: Insider Treat

Even though members of our workforce have been determined to be trustworthy custodians of classified or proprietary information, this does not make them immune to the human condition. Life happens, and we all have to deal with challenges, crises, and the obstacles that life will inevitably present.

Reporting

Screen 4 of 28

Narration: Because we understand "life happens" to all of us, people are often reluctant to report suspicious behavior, even where there is reasonable evidence that something is not right. They don't want to pry into other people's business, or they are afraid of making false accusations. It's natural to want to give someone the "benefit of the doubt," especially when it's someone in a position of authority, a colleague, or a friend.

Screen text: Insider Threat

Because we understand "life happens" to all of us, people are often reluctant to report suspicious behavior, even where there is reasonable evidence that something is not right.

They don't want to pry into other people's business, or they are afraid of making false accusations. It's natural to want to give someone the "benefit of the doubt," especially when it's someone in a position of authority, a colleague, or a friend.

Insider Threat Definition

Screen 5 of 28

Narration: The stakes are simply too high NOT to report incidents of possible insider threat as soon as they occur. Please review the definitions for insider and insider threat on screen.

Screen text: The stakes are simply too high **NOT** to report incidents of possible insider threat as soon as they occur. DoD Directive 5205.16 defines an “insider” as:

Any person with authorized access to DoD resources by virtue of employment, volunteer activities, or contractual relationship with DoD. This can include employees, former employees, consultants, and anyone with access.

The National Insider Threat Task Force (NITTF) defines an “insider threat” as:

The threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of department resources or capabilities.

Betrayed Video

Screen 6 of 28

Audio:
ANDY: Let me just tell you what I know. I'm concerned about a highly classified report that I found on incubating animal Orthopoxviruses. It's produced by GYR Biotech, it's a private company working for a defense contractor. I have it all outlined there on page 3.
On July 27th, Doug contacted me about obtaining that report.
INVESTIGATOR 1: Why you?
ANDY: I had connections there. I used to be their security liaison.
INVESTIGATOR 1: Did he say why he needed it?
ANDY: For an investigation, he didn't specify. I just assumed that it was a need-to-know basis and I guess I didn't need to know.
GAYLE: But the thing I'm really beating myself up over, I thought I caught him photographing documents with his cell phone.
GAYLE: Hey Doug! What are you doing?
DOUG: Uh, texting my attorney about the divorce papers, they're due today. Except my thumbs are too fat to type it out. I know busted. Cell phones in the SCIF.
GAYLE: I’ll let it go this time.

DOUG: Thanks.
GAYLE: A couple times a week he'd sign on with a level 7 dwarf named Dagon or a level 4 druid named Hannuuh. Sometimes he'd be on with both of them. I thought maybe they were sources, but then I thought that it was just his son and someone else they were playing with. I even brought it up to Tom and Andy.
ANDY: Well, I agree he has been acting kind of strange, but do you really think he's up to something?
TOM: I think you've watched Mission Impossible one too many times. I mean I love Doug but he's just not that clever.
GAYLE: What about the way he changes screens when you step into the room? Or this hot new girlfriend of his?
TOM: So that's what this is all about?
GAYLE: Screw you, Tom!
TOM: Hey, this is between him and Karen, it's none of our business.
ANDY: Oh come on, Tom. She's way to good looking for him. Do you think that you could get a girl like that?
TOM: I would if I could, more power to him.
GAYLE: I think I caught him photographing documents.
ANDY: What?
GAYLE: He was holding his cell phone over them and pushing buttons, but he said he was just trying to text. We can't take the chance.
TOM: Hey this is Doug we're talking about.
GAYLE: He's changed.
TOM: It's the divorce.
GAYLE: It's our responsibility to call the security officer.
TOM: Uh uh, no way!
GAYLE: It's all confidential. If there's nothing there no one will ever know. It won't even show up in his file.
TOM: In law enforcement, you trust your partner.
GAYLE: Well in intelligence you err on the side of your country.
TOM: Are you saying I don't love my country?
ANDY: OK, let's just cool down.
TOM: Hey, Doug has always had my back. I'm not diming him out over some vague suspicions. I mean, you got a problem with some of things that he's been doing. Great, be up front with him! We owe him that much at least.
GAYLE: But that's not the way we handle it in our world, and you know that.
GAYLE: Andy sided with Tom. Tom went over and talked to him and told him how things looked.
INVESTIGATOR 1: Letting the fox know when the hens are sleeping.
This time we got lucky...spooked Collins into making the drop that brought him down.
INVESTIGATOR 2: How did you learn about his trip to London?
GAYLE: It was at a baby shower of a mutual friend. Karen was there.
KAREN: I can't get him to co-sign his son's college loan and he's behind on his child support but he has the money to take his girlfriend to London.

GAYLE: He went to London?
KAREN: Yeah, with his girlfriend.
GAYLE: He never mentioned it. Usually, we know when someone in our unit has authorized foreign travel. So I went home and did some research. I found this picture of Doug and Gita on her social network page. "I know that sign." *typing*
GAYLE: There was a sign from the London underground right behind them. I had no way of knowing whether it was authorized or not or if there was anything to my other suspicion. *dialing phone* *phone ringing*
GAYLE: Hey Larry, it's Gayle Stewart. I'm sorry for calling so late. I have something I need to talk to you about.

Questions to Consider

Screen 7 of 28

Narration: After viewing that video, consider the following questions.

Screen text: Betrayed
The Trusted Insider

Questions to Consider:

- What specific insider threat indicators did the team members observe?
- What excuse(s) did each team member use to explain away the insider threat?
- At what point should each member of the team have taken action and contacted their security officer?
- At what point would you have?

Categories

Screen 8 of 28

Narration: The NITTF defines five main categories of insider threat which we will discuss in this course: leaks, spills, espionage, sabotage, and targeted violence.

Screen text: Categories

The NITTF defines five main categories of insider threat which we will discuss in this course:

- LEAKS
- SPILLS
- ESPIONAGE
- SABOTAGE
- TARGETED VIOLENCE

Leaks

Screen 9 of 28

Narration: Leaks are the intentional, unauthorized disclosure of classified or proprietary information to a person or an organization that does not have a "need-to-know." Here's an example where a Nintendo employee, who had access to a camera and an unreleased version of the game Super Smash Brothers, leaked game information to the public. Continue reading for more information on this leak.

Screen text: Categories - Leaks

Leaks are the intentional, unauthorized disclosure of classified or proprietary information to a person or an organization that does not have a "need-to-know."

Example: **Nintendo Gets Attacked From The Inside**

A Nintendo employee who had access to a camera and an unreleased version of the game Super Smash Brothers, leaked game information to the public.

Posting anonymously on 4chan's video games board, the leaker shared images of multiple unconfirmed characters along with screenshots of different game modes that hadn't yet been shown to the public. At first, the leak was deemed to be a hoax due to the outrageous claim that one of the characters was the dog from the popular 80's game Duck Hunt. But within hours, the leaker had posted videos of themselves playing as all of the characters that had yet to be announced, along with pictures of different collectibles that didn't make it into the main game. There are unconfirmed reports that Nintendo had figured out which employee leaked all of this sensitive information and had dealt with them.

Rollover text:
Hoax: see Resources for link.

Harry Potter Leak

Screen 10 of 28

Narration: Let's look at another example.

Screen text: Categories - Leaks

Example: **Harry Potter and the Tale of $20 million down the Drain.**

With the release of the final Harry Potter book on the horizon, tensions were high in the Bloomsbury offices. After dealing with nightmarish leaks a few years prior, where people actually took time out of their day to ruin the story for others by yelling out death spoilers for

Harry Potter and the half-Blood Prince in public before the book's release, Bloomsbury wasn't taking any chances on letting the final book in the series be spoiled in the same manner.

In an attempt to block spoilers and leaks, the company proceeded to spend upward of $20 million on security measures for the book shipments going out to retailers and threaten any store that even dared to open the containers holding the precious books. In the end, this was all for nothing, as someone managed to get a copy of the book days before its release. The person proceeded to take pictures of every single page in the book and post them online for all to see. The big finale was spoiled, and Bloomsbury was out a huge chunk of money for its troubles.

Rollover text:
Death Spoilers: see Resources for link.

Spills

Screen 11 of 28

Narration: Spills are the unintentional transfer of classified or proprietary information to unaccredited or unauthorized systems, individuals, applications, or media. Spills are the most common form of insider threat. They don't have to have malicious intent to cause damage. Most people think of data spills from computer systems or over the internet. Spills, however, are not limited to the cyber realm. They can occur when a book is published or when a public presentation or interview is given.

Screen text: Categories - Spills

Spills are the unintentional transfer of classified or proprietary information to unaccredited or unauthorized systems, individuals, applications, or media.

Spills are the most common form of insider threat. They don't have to have malicious intent to cause damage. Most people think of data spills from computer systems or over the internet. Spills, however, are not limited to the cyber realm. They can occur when a book is published or when a public presentation or interview is given.

Espionage

Screen 12 of 28

Narration: Espionage is the unauthorized transmittal of classified or proprietary information to a competitor, foreign nation, or entity with the intent to harm. Gregory Allen Justice was convicted of economic espionage for selling sensitive satellite information to a person he believed to be an agent of a Russian intelligence service. Justice sought and received thousands of dollars in cash payments in exchange for the materials he was providing.

Screen text: Categories - Espionage

Espionage is the unauthorized transmittal of classified or proprietary information to a competitor, foreign nation, or entity with the intent to harm.

Example: Gregory Allen Justice was convicted of economic espionage for selling sensitive satellite information to a person he believed to be an agent of a Russian intelligence service. Justice was an engineer working for a cleared defense contractor. Specifically, he worked on military and commercial satellite programs.

In exchange for providing these materials during a series of meetings between February and July of 2016, Justice sought and received thousands of dollars in cash payments. During one meeting, Justice discussed developing a relationship like the one depicted on the television show "The Americans", and during their final meeting, he offered a tour of his employer's production facilities where Justice said all military spacecraft were built.

Rollover text:
The Americans: The Americans is a period drama about the complex marriage of two KGB spies posing as Americans in suburban Washington, D.C. during the Reagan administration.

Sabotage

Screen 13 of 28

Narration: Sabotage means to deliberately destroy, damage, or obstruct, especially for political or military advantage. For example: A systems administrator granted developer testers local administrative access on their system. The testers created five additional administrator accounts, which were never noticed, and back doors were created into the different databases. When one of the developers found out he was going to be fired, he accessed the system through one of the back doors and shut the system down.

Screen text: Categories - Sabotage

Sabotage means to deliberately destroy, damage, or obstruct, especially for political or military advantage. Although sabotage is often conducted for political or military reasons, other motivations can include personal disgruntlement.

Example: A systems administrator granted developer testers local administrative access on their system. The testers created five additional administrator accounts, which were never noticed, and back doors were created into the different databases. When one of the developers found out he was going to be fired, he accessed the system through one of the back doors and shut the system down.

Targeted Violence

Screen 14 of 18

Narration: Targeted Violence represents any form of violence that is directed at an individual or group, for a specific reason. In other words, targeted violence is not a random act. Here's an example: An employee overheard his coworker make a threatening statement involving a firearm. The coworker was reported to have been upset regarding an issue that occurred in the workplace, and made the comment, "If I had a gun, I would shoot them." Following an investigation, the coworker admitted to making those remarks and stated that he did not intend to act on the comment he made. The coworker admitted to having a temper, but had no intentions of shooting anyone.

Screen text: Categories – Targeted Violence

Targeted Violence represents any form of violence that is directed at an individual or group, for a specific reason. In other words, targeted violence is not a random act.

Example: An employee overheard his coworker make a threatening statement involving a firearm. The coworker was reported to have been upset regarding an issue that occurred in the workplace, and made the comment, "If I had a gun, I would shoot them."

Following an investigation, the coworker admitted to making those remarks and stated that he did not intend to act on the comment he made. The coworker admitted to having a temper, but had no intentions of shooting anyone.

Categories of Targeted Violence

Screen 15 of 28

Narration: Listed are the categories of Targeted Violence.

Screen text: Categories – Targeted Violence

The categories of Target Violence include:

- Active Shooter
- Domestic Violence
- Harassment
- Hostile Work Environment
- Sexual Assault
- Stalking
- Threats/Threatening Behavior
- Workplace Bullying/Violence

Active Shooter

Screen 16 of 28

Narration: An active shooter is a person actively engaged in killing, or trying to kill, people in a confined and populated area. Active shooters are not limited only to the use of guns. View the example.

Screen text: Categories – Targeted Violence

An active shooter is a person actively engaged in killing, or trying to kill, people in a confined and populated area. Active shooters are not limited only to the use of guns.

Example: **Disgruntled former employee kills 5 at workplace neat Orlando**:

Five people were shot and killed by a "disgruntled" former employee at a workplace near Orlando, Florida, three years after the suspect was involved in another workplace violence incident there.

John Robert Neumann shot and killed himself after shooting his former co-workers at Fiamma, which is part of an Italian company that manufactures awnings and accessories for RVs, authorities said.

Most of the victims were shot in the head and some were shot multiple times.

Domestic Violence

Screen 17 of 28

Narration: Domestic Violence refers to violence, usually in the form of physical abuse or threat that creates a risk to the health and safety of an employee or multiple employees. Domestic violence includes any abusive, violent, coercive, forceful, or threatening act or word used to gain power and control over a household or family member, current or former spouse, current or former intimate partner, current or former dating partner, or co-parent. This behavior includes, but is not limited to physical or sexual violence, emotional or psychological intimidation, verbal abuse, stalking, economic control, harassment, threats, physical intimidation, or injury. View the example.

Screen text: Categories – Targeted Violence

Targeted Violence: Domestic Violence

Domestic Violence refers to violence, usually in the form of physical abuse or threat that creates a risk to the health and safety of an employee or multiple employees.

Domestic violence includes any abusive, violent, coercive, forceful, or threatening act or word used to gain power and control over a household or family member, current or former spouse, current or former intimate partner, current or former dating partner, or co-parent. This behavior includes, but is not limited to physical or sexual violence, emotional or psychological intimidation, verbal abuse, stalking, economic control, harassment, threats, physical intimidation, or injury.

Example: An employee reported that she was the victim of domestic violence by her former spouse. The employee provided pictures showing bruises, text messages, and documentation of the abuse. The spouse did not work at the same company.

Human Resources was able to coordinate with the local police department to provide the employee with contact information/guidance to file a protective order against her spouse.

Harassment

Screen 18 of 28

Narration: Harassment is any unwelcome written, verbal, or physical conduct that objectively creates a hostile or offensive work environment. Harassment may or may not be based on age, color, gender, mental or physical disabilities, national origin, race, religion, genetic information, sexual orientation, parental status, or reprisal (that is, for opposing employment discrimination and/or for participating in the EEO complaint process). View the on screen example.

Screen text: Categories - Targeted Violence

Targeted Violence: Harassment

Harassment is any unwelcome written, verbal, or physical conduct that objectively creates a hostile or offensive work environment. Harassment may or may not be based on age, color, gender, mental or physical disabilities, national origin, race, religion, genetic information, sexual orientation, parental status, or reprisal (e.g., for opposing employment discrimination and/or for participating in the EEO complaint process).

Example: Employee 1 reported that Employee 2 was bullying, harassing, and picking on him for not including himself in an office conversation. It was reported that Employee 2 had outbursts of anger and threatened Employee 1.

After a thorough investigation, management removed Employee 2 from the office workspace, and referred him to Human Resources. Employee 1 confirmed there were not further issues once Employee 2 was removed from the workspace.

Hostile Work Environment

Screen 19 of 28

Narration: Behaviors that create a hostile work environment include severe or pervasive actions or those that are perceived as unwelcome. View the example.

Screen text: Categories – Targeted Violence

Targeted Violence: Hostile Work Environment

Behavior or actions that create a hostile work environment are:

- Severe or persuasive
- Perceived as unwelcome or offensive

Example: An employee reported that one of her colleagues was the cause of a hostile work environment. The employee stated that the coworker had numerous anger outbursts, caused conflicts in the office, and treated other colleagues unfairly thus creating a hostile work environment. This coworker reportedly threw office objects and yelled obscenities.

After a thorough investigation, the employee was reassigned to another department.

Sexual Assault

Screen 20 of 28

Narration: Sexual Assault refers to a range of behaviors including, but not limited to, a completed nonconsensual sex act (for example, rape, sodomy, and child molestation), an attempted nonconsensual sex act, and/or abusive sexual contact. Sexual assault includes any sexual act or behavior perpetrated upon another without that person's consent or when they cannot consent. Lack of consent should be inferred when an alleged perpetrator uses force, threat of force, threat of an adverse personnel or disciplinary action, or other coercion, or when the victim is asleep, incapacitated, unconscious, or physically or legally incapable of consent. View the on screen example.

Screen text: Categories – Targeted Violence

Targeted Violence: Sexual Assault

Sexual Assault refers to a range of behaviors including, but not limited to, a completed nonconsensual sex act (e.g., rape, sodomy, and child molestation), an attempted nonconsensual sex act, and abusive sexual contact.

Sexual assault includes any sexual act or behavior perpetrated upon another without that person's consent or when they cannot consent, whether due to incapacitation, minority (age), mental state, or physical condition.

Lack of consent should be inferred when an alleged perpetrator uses force, threat of force, threat of an adverse personnel or disciplinary action, or other coercion, or when the victim is asleep, incapacitated, unconscious, or physically or legally incapable of consent.

Example: Two employees participated in a happy hour function after work which included a significant amount of alcohol consumption.

After the work function, Employee 2 offered to take Employee 1 to her residence wherein Employee 2 attempted to force his way into the residence. Employee 1 stated that this behavior was unwanted and pushed Employee 2 away. Employee 2 ignored Employee 1's request and attempted to sexually assault Employee 1.

Employee 1 was able to push him away and secured herself in the residence. Employee 2 eventually left the residence, and the behavior was reported.

Stalking

Screen 21 of 28

Narration: Stalking refers to harassment, unwanted, or threatening physical, verbal, written, or virtual conduct that causes the victim, or could cause the victim, to fear for his or her safety or the safety of a family member or others. Stalking may include but is not limited to: Spying on a victim, making threats to harm the victim, posting rumors about the victim, and following the victim.

Screen text: Categories – Targeted Violence

Targeted Violence: Stalking

Screen text: Stalking refers to harassment, unwanted, or threatening physical, verbal, written, or virtual conduct that causes the victim, or could cause the victim, to fear for his or her safety or the safety of a family member or others. Stalking may include but is not limited to, the following:

- Spying on, or waiting for the victim in places such as home, school, work, or recreation place
- Leaving unwanted items, presents, or flowers for the victim
- Making direct or indirect threats to harm the victim, the victim's children, relatives, friends, intimate partners, pets or property
- Posting information or spreading rumors about the victim on the internet, in a public place, or by word of mouth
- Obtaining personal information about the victim by accessing public records, using internet search services, hiring private investigators, going through the victim's garbage, following the victim, or contacting their friends, family, work, or neighbors

Threatening Behavior

Screen 22 of 28

Narration: Threatening behavior is any use of words or actions that may intimidate or provoke a reasonable person and/or interfere with the performance of official duties. View the example.

Screen text: Categories – Targeted Violence

Targeted Violence: Threats/Threatening Behavior

Threatening behavior is any use of words or actions that may intimidate or provoke a reasonable person and/or interfere with the performance of official duties.

Example: A company executive received threatening emails from an individual stating the company's product was harming his family. The individual stated he would seek revenge and that the executive would suffer for his actions.

Workplace Bullying

Screen 23 of 28

Narration: Workplace bullying/violence is intentional, disruptive physical, verbal, or written behavior committed by an individual or group that physically damages a facility, or psychologically or physically abuses/harms/violates the safety and well-being of an employee or persons associated with the company. View the example of workplace bullying.

Screen text: Categories – Targeted Violence

Targeted Violence: Workplace Bullying/Violence

Workplace bullying/violence is intentional, disruptive physical, verbal, or written behavior committed by an individual or group that physically damages a facility, or psychologically or physically abuses/harms/violates the safety and well-being of an employee or persons associated with the company.

Example: Two employees were working on a project together. It was reported that Employee 1 was assaulted by Employee2.

Employee 1 said profanities towards Employee 2. Employee 2 took offense, choking Employee 1 and pushing him.

Management contacted Security and removed Employee 2's access to the company facilities and systems.

Knowledge Check 1

Screen 24 of 28

Screen text: Knowledge Check

1. What is the name for the unintentional transfer of classified or proprietary information to unaccredited or unauthorized systems, individuals, applications, or media?
   ○ Espionage

   ○ Sabotage ○

   Spill ○ Leak

Knowledge Check 2

Screen 25 of 28

Screen text: Knowledge Check

2. What Targeted Violence subcategory results in physical or psychological harm to the safety and well-being of an employee? ○ Leak
   ○ Workplace Bullying/Violence

   ○ Sabotage ○ Espionage

Knowledge Check 3

Screen 26 of 28

Screen text: Knowledge Check

3. What is the name for the intentional, unauthorized disclosure of classified or proprietary information to a person or an organization that does not have a "need-to-know"? ○ Leak
   ○ Workplace Bullying/Violence

   ○ Sabotage ○ Espionage

Summary

Screen 27 of 28

Narration: In this lesson, you learned the definition of insiders and insider threat. You also learned about the five categories of insider threat and the subcategories of Targeted Violence. In the next lesson, you will learn about potential vulnerabilities and behavioral indicators that might lead to someone becoming an insider threat.

Screen text: Summary

In this lesson, you learned the definition of insiders and insider threat. You also learned about the five categories of insider threat and the subcategories of Targeted Violence. In the next lesson, you will learn about potential vulnerabilities and behavioral indicators that might lead to someone becoming an insider threat.

Lesson Completion

Screen 28 of 28

Narration: Congratulations! You have completed Lesson 1.

Screen text: Congratulations! You have completed Lesson 1

LESSON 01 INSIDER THREAT CATEGORIES

Lesson 2

Indicators

Introduction

Screen 1 of 27

Narration: In this lesson, you will learn about potential vulnerabilities and behavioral indicators that relate to the insider threat.

Screen text: Lesson 02/Introduction

No one is immune to vulnerabilities and the difficult situations that confront us at various times in our lives.

- Adversaries look for vulnerabilities to exploit
- In some instances, vulnerabilities motivate us to consider doing something that makes us an insider threat

In this lesson, you will learn about potential vulnerabilities and behavioral indicators that relate to the insider threat.

Learning Objectives

After completing this lesson, you will be able to:

- Identify potential insider threat vulnerabilities by cleared employees
- Describe insider threat behavioral indicators

Vulnerabilities

Screen 2 of 27

Narration: We all have vulnerabilities. But not everyone who exhibits vulnerabilities represents a potential insider threat. However, some vulnerabilities could increase the risk that an insider could be exploited or make the decision to leak, commit espionage, or engage in sabotage and/or targeted violence.

Screen text: Vulnerabilities

We all have vulnerabilities. Not everyone who exhibits vulnerabilities represents a potential insider threat.

However, some vulnerabilities could increase the risk that an insider could be exploited or make the decision to leak, commit espionage, or engage in sabotage and/or targeted violence.

Examples of Vulnerabilities

Screen 3 of 27

Narration: Some examples of vulnerabilities include financial stress, addictive behaviors, and disgruntlement.

Screen text: Vulnerabilities

Examples of vulnerabilities include:

- Financial stress
- Exploitable promiscuity
- Addictive behaviors (e.g., drug/alcohol abuse, gambling, pornography)
- Loneliness
- Disgruntlement

Respect

Screen 4 of 27

Narration: Seeking assistance to help deal with life's challenges is not a sign of weakness. In fact, it's a sign of good judgement and an act of bravery to say, "I need help." Identifying colleagues who may be in need of help is not an act of betrayal. It is an ultimate act of respect; respect for the safety and well-being of the individual, for the company, and for the nation.

Screen text: Vulnerabilities

Seeking assistance to help deal with life’s challenges is not a sign of weakness. In fact, it’s a sign of good judgement and an act of bravery to say, "I need help."

Identifying colleagues who may be in need of help is not an act of betrayal. It is an ultimate act of respect; respect for the safety and well-being of the individual, for the company, and for the nation.

Stories

Screen 5 of 27

Narration: Let’s meet some people who exhibit vulnerabilities and see how their stories play out…

Screen text: Let’s meet some people who exhibit vulnerabilities and see how their stories play out.

Financial Stress

Screen 6 of 27

Narration: Here’s an example of financial stress. Sarah, recently divorced, is the single parent of a four-year-old with special needs. She requested to be assigned near a major medical facility so she can ensure that her son gets the best care. She isn’t receiving much financial help from her son’s father and having to move is causing additional financial hardships. Her babysitter, Crystal, said that she has a friend willing to lend Sarah enough money to pay her bills.

Screen text: Vulnerabilities/Financial Stress

Sarah, recently divorced, is the single parent of a four-year-old with special needs. She requested to be assigned near a major medical facility so she can ensure that her son gets the best care. She isn’t receiving much financial help from her son’s father and having to move is causing additional financial hardships.

Her babysitter, Crystal, said that she has a friend willing to lend Sarah enough money to pay her bills.

Financial Stress (cont.)

Screen 7 of 27

Narration: Many companies have an Employee Assistance Program, or EAP, that offers financial counseling services that will help you establish a plan to achieve financial stability. In the on screen example, Sarah’s EAP averted a potential problem.

Screen text: Vulnerabilities/Financial Stress/Financial Help

Many companies have an Employee Assistance Program (EAP) that offers financial counseling services that will help you establish a plan to achieve financial stability.

Financial Vulnerability Exploitation Averted

Sarah, buckling under financial pressure, shared her concerns with her supervisor, Jill. She also told Jill about the loan offer from Crystal's friend.

Jill thought the offer sounded suspicious and advised Sarah to decline the offer. She directed Sarah to the EAP for financial counseling to help her get back on track to prepare for the move.

Exploitable Promiscuity

Screen 8 of 27

Narration: Here's an example of exploitable promiscuity. When Harley was in college, he had a somewhat promiscuous and wild social life. Since then, he has matured into a highly-regarded employee. Unfortunately, there is evidence of his former life on the Internet. His college buddy, George, recently contacted Harley out of the blue. George said that he and another friend were laughing at the Facebook photos of Harley in his "wild" years and thought to contact him. During the conversation, George explained that he had fallen on hard times and was wondering if Harley could help him find a job or lend him some money.

Screen text: Vulnerabilities/Exploitable Promiscuity

When Harley was in college, he had a somewhat promiscuous and wild social life. Since then, he has matured into a highly-regarded employee.

Unfortunately, there is evidence of his former life on the Internet.

His college buddy, George, recently contacted Harley out of the blue. George said that he and another friend were laughing at the Facebook photos of Harley in his "wild" years and thought to contact him.

During the conversation, George explained that he had fallen on hard times and was wondering if Harley could help him find a job or lend him some money.

People Change

Screen 9 of 27

Narration: Harley told George that he was sorry that life was difficult for him. He encouraged George to keep looking for work and suggested a few employment programs. Harley said that he had changed a lot since those college days. He felt fortunate to have supportive people in his personal and professional life who accepted him and his past. He no longer engaged in wild antics and didn't believe in lending money.

Screen text: Vulnerabilities/Exploitable Promiscuity
People Change

Harley told George that he was sorry that life was difficult for him. He encouraged George to keep looking for work and suggested a few employment programs.
Harley said that he had changed a lot since those college days. He felt fortunate to have supportive people in his personal and professional life who accepted him and his past.

He no longer engaged in wild antics and didn't believe in lending money.

Alcohol Abuse

Screen 10 of 27

Narration: Here's an example of alcohol abuse. Bob works with a great team. In fact, he and his supervisor, Mark, are good friends. They often go to happy hour on Fridays after work. Lately, Bob has noticed an increase in Mark's drinking. What used to be a couple of beers has turned into closing the bar. On two occasions Bob had to escort Mark home because he was too drunk to drive. Bob also suspects Mark may be drinking at work. Bob confronted him on his drinking, and Mark admitted to going overboard a few times. Mark said a few drinks relieved the pressure of having to deal with his wife's cancer treatments and told Bob not to worry about it.

Screen text: Vulnerabilities/Alcohol Abuse

Bob works with a great team. In fact, he and his supervisor, Mark, are good friends. They often go to happy hour on Fridays after work. Lately, Bob has noticed an increase in Mark's drinking. What used to be a couple of beers has turned into closing the bar. On two occasions Bob had to escort Mark home because he was too drunk to drive.

Bob also suspects Mark may be drinking at work. Bob confronted him on his drinking, and Mark admitted to going overboard a few times. Mark said a few drinks relieved the pressure of having to deal with his wife's cancer treatments and told Bob not to worry about it.

Concerning Behavior

Screen 11 of 27

Narration: Bob felt that Mark was not coping in a healthy way and remained concerned about his increased drinking. Although Bob has not had much interaction with Mark's manager, Kim, he feels the situation is too important to ignore and decides to share his concerns with her.

Screen text: Vulnerabilities/Alcohol Abuse

Report Concerning Behavior

Bob felt that Mark was not coping in a healthy way and remained concerned about his increased drinking. Although Bob has not had much interaction with Mark's manager, Kim, he feels the situation is too important to ignore and decides to share his concerns with her.

Getting Help

Screen 12 of 27

Narration: The employee's behavior was a danger to himself and those around him. Reporting his concerning behaviors protects his colleagues, their objectives, and helps him get the support he needs. Most EAP's recognize diagnosable addictive disorders as treatable illnesses. They will work with employees to utilize high-quality treatment resources to return them to full productivity. It's important that employees and their families receive the assistance they need.

Screen text: Vulnerabilities/Alcohol Abuse

Report Concerning Behavior

The employee's behavior was a danger to himself and those around him. Reporting his concerning behaviors protects his colleagues, their objectives, and helps him get the support he needs.

Getting the Help You Need

Most EAPs recognize diagnosable addictive disorders as treatable illnesses. They will work with employees to utilize high-quality treatment resources to return them to full productivity. Employee's information is dealt with sensitivity and confidentiality.

Because alcohol is a legal and socially-acceptable drug, it is a principal drug of abuse. Such abuse may interfere with an individual's health, interpersonal relationships, job performance, economic status, or ability to protect classified information. Alcohol dependence, like other addictive disorders, is chronic and progressive; it can become increasingly severe and can be fatal. Many employees and their families have been assisted in achieving comfortable long-term recovery from this illness.

Loneliness

Screen 13 of 27

Narration: Here's a case about loneliness. Paisley was new to the company, recruited right out of a private college. She comes from a very small, traditional town, and finds cities to be overwhelming. She doesn’t know anyone, and the team she works with seems too busy to even tell her what her job is. She felt very isolated and alone. The only person she’s comfortable talking to in the office is Phyllis. Paisley confided in Phyllis that she recently joined an online dating site and made contact with Jeff. Jeff has been contacting her every day and seems very interested in getting together to find out more about her. Paisley wants to go to an upcoming ballet performance. She is thinking of asking Jeff and wanted Phyllis’ advice.

Screen text: Vulnerabilities/Loneliness

Paisley was new to the company, recruited right out of a private college. She comes from a very small, traditional town, and finds cities to be overwhelming. She doesn’t know anyone, and the team she works with seems too busy to even tell her what her job is. She felt very isolated and alone. The only person she’s comfortable talking to in the office is Phyllis. Paisley confided in Phyllis that she recently joined an online dating site and made contact with Jeff. Jeff has been contacting her every day and seems very interested in getting together to find out more about her. Paisley wants to go to an upcoming ballet performance. She is thinking of asking Jeff and wanted Phyllis’ advice.

Personal Information

Screen 14 of 27

Narration: Phyllis advised Paisley to consider her access to classified or proprietary information. She will need to mitigate her risk by being vigilant with the personal and professional details she shares.

Screen text: Vulnerabilities/Loneliness

Protecting Personal Information

Phyllis advised Paisley to consider her access to classified or proprietary information. She will need to mitigate her risk by being vigilant with the personal and professional details she shares.

Disgruntlement

Screen 15 of 27

Narration: Here’s an example of disgruntlement. Sam is nicknamed "bitter-man" by his coworkers. He tells everyone that he was cheated out of a promotion by his previous supervisor because, when they were single, Sam dated the supervisor’s wife. Sam’s current supervisor, Carla, has had several documented meetings with him about his attitude, but he continues to complain about not being promoted. Lately, Sam has been overheard threatening to take matters into his own hands unless he "gets what he deserves."

Screen text: Vulnerabilities/Disgruntlement

Sam is nicknamed "bitter-man" by his coworkers. He tells everyone that he was cheated out of a promotion by his previous supervisor because, when they were single, Sam dated the supervisor's wife.

Sam's current supervisor, Carla, has had several documented meetings with him about his attitude, but he continues to complain about not being promoted. Lately, Sam has been overheard threatening to take matters into his own hands unless he "gets what he deserves."

Disgruntlement (cont.)

Screen 16 of 27

Narration: Sam's behavior fit one of the insider threat behavioral indicators; disgruntlement to the point of retaliation. Carla reported his behavior to company security and her immediate supervisor. Later in this lesson we will provide an in-depth look at behavioral indicators.

Screen text: Vulnerabilities/Disgruntlement

Behavioral Indicators

Sam's behavior fit one of the insider threat behavioral indicators; disgruntlement to the point of retaliation. Carla reported his behavior to company security and her immediate supervisor.

Later in this lesson we will provide an in-depth look at behavioral indicators.

Addressing Vulnerabilities

Screen 17 of 27

Narration: If you notice a coworker wrestling with any of the insider threat vulnerabilities covered in this lesson, say something. As concerned employees, we all need to be on the lookout for colleagues who may be in trouble and notify the appropriate company representative who can help get the assistance they need before the situation escalates. In the next section of this lesson, we will cover what could happen if vulnerabilities are not addressed.

Screen text: You are the first line of defense.

If you notice a coworker wrestling with any of the insider threat vulnerabilities covered in this lesson, say something. As concerned employees, we all need to be on the lookout for colleagues who may be in trouble and notify the appropriate company representative who can help get the assistance they need before the situation escalates.

In the next section of this lesson, we will cover what could happen if vulnerabilities are not addressed.

Behavioral Indicators

Screen 18 of 27

Narration: There are many reportable behavioral indicators; too many to be covered in this course. This lesson will cover those related to the five categories of insider threat. Other behavioral indicators related to espionage will be covered in a later lesson. Review some of the reportable behavioral indicators that have been associated with insider threat.

Screen text: Behavioral Indicators

There are many reportable behavioral indicators; too many to be covered in this course. This lesson will cover those related to the five categories of insider threat. Other behavioral indicators related to espionage will be covered in a later lesson.

Many known insider threats have been associated with one or more of the following reportable behavioral indicators:

- Significant changes in personality, behavior, or work habits
- Substance abuse or addictive behaviors (e.g., alcohol and drug abuse/gambling)
- Considerable financial change (e.g., unexplained affluence or excessive debt)
- Disgruntled to the point of wanting to retaliate
- Disregard for security procedures and protocols
- Seeking access to classified or proprietary information and systems/technology without a "need-to-know"
- Access to facilities and/or proprietary information outside of normal work hours
- Unauthorized removal, or unnecessary copying or hoarding of classified or proprietary material

Cases

Screen 19 of 27

Narration: Let's look at some of the insider threat behavioral indicators as illustrated by some of the most publicized insider threat cases.

Screen text: Behavioral Indicators

Let's look at some of the insider threat behavioral indicators as illustrated by some of the most publicized insider threat cases.

Benjamin Bishop

Screen 20 of 27

Narration: Bishop, a 59-year-old civilian defense contractor arrested in March 2013, pleaded guilty to passing nuclear weapons secrets to a 27-year-old Chinese graduate student whom he met at an international military conference. Bishop fell hard for the graduate student and within a few months their relationship became intimate. Bishop had been caught in a HONEY TRAP. Bishop was sentenced to 87 months in prison and three years of supervised release.

Screen text: Benjamin Bishop

Ingratiation/Bonds of Affection

Bishop, a 59-year-old civilian defense contractor arrested in March 2013, pleaded guilty to passing nuclear weapons secrets to a 27-year-old Chinese graduate student whom he met at an international military conference. Bishop fell hard for the graduate student and within a few months their relationship became intimate. Bishop had been caught in a HONEY TRAP.

Bishop was sentenced to 87 months in prison and three years of supervised release.

Gregory A. Justice

Screen 21 of 27

Narration: Gregory Justice worked as an aerospace engineer on military and commercial satellite programs and was enamored with James Bond and the Americans. He was caring for a sick wife and felt unappreciated at work. Under all this pressure, the 49-year-old defense engineer attempted to sell satellite secrets to someone he believed was Russian intelligence. Justice pled guilty to federal charges on one count of attempting to commit economic espionage and one count of attempting to violate the Arms Export Control Act. He was sentenced to five years in prison.

Screen text: Gregory Allen Justice

Disgruntlement

Gregory Justice worked as an aerospace engineer on military and commercial satellite programs and was enamored with James Bond and the Americans. He was caring for a sick wife and felt unappreciated at work. Under all this pressure, the 49-year-old defense engineer attempted to sell satellite secrets to someone he believed was Russian intelligence. Justice pled guilty to federal charges on one count of attempting to commit economic espionage and one count of attempting to violate the Arms Export Control Act. He was sentenced to five years in prison.

John Neumann

Screen 22 of 27

Narration: An honorably discharged veteran, John Robert Neumann was extremely upset when he was fired from his job at a company that makes awnings for RVs and campers. So upset, that he returned to the company and opened fire killing five of his coworkers before turning the gun on himself. Neumann had a history of negative relationships with selected former coworkers, including battering another employee.

Screen text: John Neumann

Mental/Emotional Instability

An honorably discharged veteran, John Robert Neumann was extremely upset when he was fired from his job at a company that makes awnings for RVs and campers. So upset, that he returned to the company and opened fire killing five of his coworkers before turning the gun on himself. Neumann had a history of negative relationships with selected former coworkers, including battering another employee.

Violations

Screen 23 of 27

Narration: Studies of inside offenders have shown that most were known to have displayed concerning or problematic behavior before acting directly against their organization. This behavior included violations of policies, standard procedures, accepted practices, or laws that had been observed by managers, supervisors, and coworkers.

Screen text: Behavioral Indicators

Studies of inside offenders have shown that most were known to have displayed concerning or problematic behavior before acting directly against their organization. This behavior included violations of policies, standard procedures, accepted practices, or laws that had been observed by managers, supervisors, and coworkers.

Knowledge Check 1

Screen 24 of 27

Screen text: Knowledge Check

1. Which of the following is NOT an example of a potential insider threat vulnerability?
    - ○ Obesity ○ Drug/alcohol use ○ Loneliness
    - ○ Promiscuity

Knowledge Check 2

Screen 25 of 27

Screen text: Knowledge Check

2. Which of the following are examples of behavioral indicators associated with insider threat?
   - o Significant changes in personality, behavior, or work habits ○
     Disregard for security procedures and protocols
   - o Access to facilities and/or proprietary information outside of normal
     work hours ○ All of the above

Summary

Screen 26 of 27

Narration: In this lesson you learned about potential insider threat vulnerabilities and behavioral indicators. In the next lesson, you will learn about what adversaries want to know, how they try to get it, and what to report when contacted by the media.

Screen Text: Lesson 2/Summary

In this lesson you learned about potential insider threat vulnerabilities and behavioral indicators.

In the next lesson, you will learn about what adversaries want to know, how they try to get it, and what to report when contacted by the media.

Lesson Completion

Screen 27 of 27

Narration: Congratulations! You have completed Lesson 2.

Screen text: Congratulations! You have completed Lesson 2

LESSON 02 INDICATORS

Lesson 3

Adversaries

Introduction

Screen 1 of 19

Narration: Those who betray the trust placed in them are not only putting this nation's security at risk, they are also destroying the legacy that we have all worked so hard to achieve. It's both our professional and personal responsibility to make it as difficult as possible for would-be spies or leakers to succeed.

Screen text: Lesson 03 Introduction

Those who betray the trust placed in them are not only putting this nation's security at risk, they are also destroying the legacy that we have all worked so hard to achieve. It's both our professional and personal responsibility to make it as difficult as possible for would-be spies or leakers to succeed.

Learning Objectives

Screen 2 of 19

Narration: In this lesson, you will learn about what adversaries want to know, how they will try to get what they want, and what you should report when contacted by the media.

Screen text: Adversaries

In this lesson, you will learn about what adversaries want to know, how they will try to get what they want, and what you should report when contacted by the media.

Learning Objectives

After completing this lesson you will be able to:

- Discuss reporting media contact
- Identify what adversaries want to know
- Describe techniques used by adversaries to gather information and recruit insiders

Media Contact Screen

3 of 19

Narration: The definition of a member of the media has changed with the advent of the Internet. It's not only a newspaper reporter who might contact you; you could be contacted by blog and wiki representatives.

If you are contacted by a member of the media about information you are not authorized to share, you should take down the person's name and organization, date, time, location, method of contact and the reason for contact.

Report this information to your organization's security office.

Screen text: Media Contact

The definition of a member of the media has changed with the advent of the Internet. It is not only a newspaper reporter who might contact you; you could be contacted by blog and wiki representatives, academic researchers, photographers, and newspaper and TV reporters.

If you are contacted by a member of the media about information you are not authorized to share, you should take down the following details:

- The person's name and organization
- Date, time, location
- Method of contact — phone, e-mail, or personal visit
- If possible, detail the nature of the reporter's questions and/or reason for contact

This information should be reported to your organization's security office.

Although media personnel are not typically considered a threat, their actions of collecting and reporting classified/proprietary information can be just as damaging.

Protecting Information

Screen 4 of 19

Narration: Counterintelligence and security efforts at both public and private institutions are heavily focused on protecting organizations from external adversaries. They spend billions of dollars to build perimeter defenses, hire guards, and create IT firewalls to keep their enemies out.

Our society has become conditioned by the Internet, and especially social media to openly share information, whether personal or professional.

This can lead to unintentional disclosure of classified or proprietary information and make public and private sector employees more susceptible to approaches by their adversaries.

Screen text: Counterintelligence and security efforts at both public and private institutions are heavily focused on protecting organizations from external adversaries. They spend billions of dollars to build perimeter defenses, hire guards, and create IT firewalls to keep their enemies out.

Our society has become conditioned by the Internet, and especially social media to openly share information, whether personal or professional. This can lead to unintentional disclosure of classified or proprietary information and make public and private sector employees more susceptible to approaches by their adversaries.

Adversaries

Screen 5 of 19

Narration: Foreign governments, terrorist organizations, competitors, and non-state actors want to know non-public information that an insider can provide.

Public and private organizations in the United States are targeted by many foreign entities throughout the world. There are several countries which consistently present counterintelligence concerns, whose intelligence services are particularly aggressive, and adept at targeting and exploiting personal relationships.

Screen text:

Foreign governments, terrorist organizations, competitors, and non-state actors want to know non-public information that an insider can provide.

Public and private organizations in the United States are targeted by many foreign entities throughout the world. There are several countries which consistently present counterintelligence concerns, whose intelligence services are particularly aggressive, and adept at targeting and exploiting personal relationships.

What They Want to Know

Screen 6 of 19

Narration: Adversaries want to know: who are the organization's personnel; with which countries does the organization work; what are the organization's methodologies, capabilities, and limitations; and where are the organization's facilities located worldwide?

Screen text: What Adversaries Want to Know

What our adversaries want to know about public and private organizations:

- Who are the organization's personnel?
- With which countries does the organization work?
- What are the organization's methodologies, capabilities, and limitations?
- Where are the organization's facilities located worldwide?

Gathering Information

Screen 7 of 19

Narration: An adversary will go to any length to access information you and your colleagues might have. Review the techniques they will employ to try to get this information.

Screen text:
An adversary will go to any length to access information you and your colleagues might have. There are techniques they will employ to try to get this information.

Direct Approach

- Approaches during travel
- Persistent requests to socialize
- If presenting at a conference, requests for presentation materials months in advance

Exploitation

- Excessive photography or videotaping
- Concealed listening devices
- Malicious emails
- Unsecured Wi-Fi

Elicitation

Screen 8 of 19

Narration: Elicitation is a technique used to discreetly gather information. It's a conversation with a specific purpose to collect information that is not readily available and do so without raising suspicion. The conversation can be in person, over the phone, or in writing and will appear to be social or professional conversation.

Competitive business intelligence collectors and foreign intelligence officers are trained in elicitation tactics. Their job is to obtain non-public information.

A business competitor may want information to out-compete your company, or a foreign intelligence officer may want insider information or details on national security information or U.S. defense technologies.

Screen text: Elicitation

Elicitation is a technique used to discreetly gather information. It is a conversation with a specific purpose:

Collect information that is not readily available and do so without raising suspicion.

The conversation can be in person, over the phone, or in writing. It will appear to be normal social or professional conversation. Many competitive business intelligence collectors and foreign intelligence officers are trained in elicitation tactics. Their job is to obtain non-public information. A business competitor may want information to out-compete your company, or a foreign intelligence officer may want insider information or details on national security information or U.S. defense technologies.

Why Elicitation Works

Screen 9 of 19

Narration: A trained elicitor understands certain human or cultural predispositions and uses techniques to exploit them. Review the natural tendencies an elicitor may try to exploit.

Screen text: Why Elicitation Works

A trained elicitor understands certain human or cultural predispositions and uses techniques to exploit them. Natural tendencies an elicitor may try to exploit include:

- A desire to be polite and helpful, even to strangers
- A desire to appear well-informed
- A desire to feel appreciated and believe we are contributing something important
- A tendency to expand on a topic when given praise or encouragement; to show off
- A tendency to gossip
- A tendency to correct others
- A tendency to underestimate the value of the information being sought or given, especially if we are unfamiliar with how else that information could be used
- A tendency to believe others are honest; a disinclination to be suspicious of others
- A tendency to answer truthfully when asked an "honest" question
- A desire to convert someone to our opinion

Example of Elicitation

Screen 10 of 19

Narration: You meet someone at a public function and the natural getting-to-know-you questions eventually turn to work. You never mention the name of your organization. The new person asks questions about job satisfaction at your company, perhaps while complaining about his job.

However, he may know exactly what you do but relies on his anonymity, your desire to be honest and appear knowledgeable, and your disinclination to be suspicious to get the information he wants.

He may be hunting for a disgruntled employee who he can entice to give him insider information.

Screen text: Example of Elicitation

Here’s a short example of elicitation:

You meet someone at a public function and the natural getting-to-know-you questions eventually turn to work. You never mention the name of your organization.

The new person asks questions about job satisfaction at your company, perhaps while complaining about his job.

However, he may know exactly what you do but relies on his anonymity, your desire to be honest and appear knowledgeable, and your disinclination to be suspicious to get the information he wants. He may be hunting for a disgruntled employee who he can entice to give him insider information.

Techniques

Screen 11 of 19

Narration: Since the end of the Cold War: 67% of spies have been civilians, 84% of spies were successful, 40% were caught immediately or in less than one year, 81% received no money for their services, and 94% went to prison.

Screen text: Do These Techniques Work?

Since the end of the Cold War (1991):

- 67% of spies have been civilians
- 37% had no security clearance
- 84% of spies were successful
- 40% were caught immediately or in less than one year
- 19% were active for five or more years
- 67% volunteered to commit espionage
- 81% received no money for their services
- 94% went to prison

Source: Raytheon's pamphlet "What Employees Should Know About Elicitation and Foreign Intelligence Approaches"

$300,000,000,000 worth of American intellectual property and business intelligence are stolen yearly by China, Russia, Iran, and others.

Do These Techniques Work?

Screen 12 of 19

Narration: A 59-year-old civilian defense contractor pled guilty to giving classified nuclear weapons information to a 27-year-old Chinese graduate student whom he had met at an international military conference.

In Louisiana, a naturalized U.S. citizen with 27 years of service, working for a U.S. chemical company, conspired with former colleagues and overseas partners to steal a specific formula and market that technology to companies in his native country.

Recent conference badges contained a microphone, LED, digital signal processor, and a custom circuit board.

At the University of Wisconsin-Madison, a research assistant was convicted of shipping samples of a cancer treatment to his home country to start his own research center to develop and market the drug.

Screen text: Do These Techniques Work?

A 59-year-old civilian defense contractor plead guilty to giving classified nuclear weapons information to a 27-year-old Chinese graduate student whom he met at an international military conference.

In Louisiana, a naturalized U.S. citizen with 27 years of service, working for a U.S. chemical company, conspired with former colleagues and overseas partners to steal a specific formula and market that technology to companies in his native country.

Recent conference badges contained a microphone, LED, digital signal processor, and a custom circuit board.

At the University of Wisconsin-Madison, a research assistant was convicted of shipping samples of a cancer treatment to his home country to start his own research center to develop and market the drug.

What to Do?

Screen 13 of 19

Narration: What are some ways to reduce the chance of inadvertently revealing classified or proprietary information to an adversary? Be prepared, beware of odd behaviors, and reduce exploitation.

Screen text: What Should You Do?

What are some ways to reduce the chance of inadvertently revealing classified or proprietary information to an adversary?

Be Prepared

- Talk to your local security officer
- Research local environment, your destination, and any conference venue and attendees

Beware of Odd Behaviors

- Watch for repeat requests or multiple approaches
- Check if acquired business cards match a real company

- Practice situational awareness

Reduce Exploitation

- Use Wi-Fi only with a Virtual Private Network
- Screen/review suspicious emails and texts
- Don’t loan your devices to anyone or let them plug into your devices
- Don’t use unknown computers, faxes, or phones for sensitive discussions

Deflecting Elicitation Attempts

Screen 14 of 19

Narration: There are ways to deflect elicitation attempts. You should know what information not to share and be suspicious of people who seek such information.

Do not give out any unauthorized information including personal information about you, your family, or your colleagues.

You can politely discourage conversation topics and deflect possible elicitations by referring them to public sources, giving a nondescript answer, or stating you cannot discuss the matter.

Screen text: Deflecting Elicitation Attempts

How can you deflect elicitation attempts?

Know what information should not be shared and be suspicious of people who seek such information. Do not give out any unauthorized information including personal information about you, your family, or your colleagues.

You can politely discourage conversation topics and deflect possible elicitations by:

- Referring them to public sources (websites, press releases)
- Ignoring any questions or statements you think are improper and changing the topic
- Deflecting a question with one of your own
- Responding with, "Why do you ask?"
- Giving a nondescript answer
- Stating that you do not know
- Stating that you would have to clear such discussions with your security office
- Stating that you cannot discuss the matter

If you see something, say something!

If you believe someone has tried to elicit information from you, especially about your work, report it to your organization’s security office.

Knowledge Check 1

Screen 15 of 19

Screen text: Knowledge Check

1. True or False? Adversaries only target you if you have a security clearance.
   - ○ True ○ False

Knowledge Check 2 Screen

16 of 19

Screen text: Knowledge Check

2. True or False? You Adversaries only target you if you have a security clearance.
   - ○ True ○ False

Knowledge Check 3

Screen 17 of 19

Screen text: Knowledge Check

3. Which of the following is NOT a way to deflect an elicitation attempt?
   - ○ Ignoring any questions or statements you

     think are improper and changing the topic ○

     Tell them what they want to know up front ○

     Stating that you do not know
   - ○ Deflecting a question with one of your own

Summary

Screen 18 of 19

Narration: This lesson covered what adversaries want to know, how they try to get it, and what you should report when contacted by the media. In the next lesson, you will learn how advances in technology impact the insider threat.

Screen text: Summary

This lesson covered what adversaries want to know, how they try to get it, and what you should report when contacted by the media.

In the next lesson, you will learn how advances in technology impact the insider threat.

Lesson Completion

Screen 19 of 19

Narration: Congratulations! You have completed Lesson 3.

Screen text:

Congratulations!
You have completed Lesson 3

LESSON 03 ADVERSARIES

Lesson 4: Technology

Introduction

Screen 1 of 18

Narration: In this lesson, you will learn how adversaries take advantage of advances in technology, about the ease with which information can be accessed and transferred, and about your role in mitigating this threat.

Review the lesson learning objectives.

Screen text: In this lesson, you will learn how adversaries take advantage of advances in technology, about the ease with which information can be accessed and transferred, and about your role in mitigating this threat.

Learning Objectives

After completing this lesson, you will be able to:

- Describe how advances in technology impact the insider threat
- List some indicators of possible technology-related insider threat
- Describe vulnerabilities posed by using social networking services
- Describe how your help can reduce the technology-associated insider threat

Technology

Screen 2 of 18

Narration: Thanks to rapid advances in technology, the world is more interconnected than ever before. While this heightened connectivity enriches our lives, it comes with a cost.

As our connectivity increases, so do a myriad of persistent and potentially grave technologyrelated threats.

These threats present new counterintelligence and security challenges in protecting classified and proprietary information from unauthorized access or improper use by a trusted insider.

Screen text: Lesson 04 Introduction

Thanks to rapid advances in technology, the world is more interconnected than ever before. While this heightened connectivity enriches our lives, it comes with a cost.
As our connectivity increases, so do a myriad of persistent and potentially grave technologyrelated threats. These threats present new counterintelligence and security challenges in protecting classified and proprietary information from unauthorized access or improper use by a trusted insider.

Computer Technology Screen

3 of 18

Narration: In today's high-tech world, one individual can do extraordinary damage. Both spies and leakers have exploited computer technology to obtain and transfer vast amounts of classified data. Using their position, trusted insiders can damage or disrupt an organization's activities.

Technology changes the scale of the risk of information loss through insider threat.

Screen text: Lesson 04 Introduction

In today's high-tech world, one individual can do extraordinary damage. Both spies and leakers have exploited computer technology to obtain and transfer vast amounts of classified data. Using their position, trusted insiders can damage or disrupt an organization's activities and operations; destroy, steal, or alter equipment; install malware; and facilitate access for an adversary to conduct a technical operation.

Technology changes the scale of the risk of information loss through insider threat. Where once insiders were limited to what they could print and carry out of a facility, technical devices allow insiders to get much more data than they could print.

Timeline

Screen 4 of 18

Narration: The more technology advances, the more challenging information protection becomes, in part because storage capacity has increased. Aldrich Ames was found to have four floppy disks containing classified information.

When arrested, James Nicholson was carrying two floppies containing classified information.

Current technology allows even more data to be accessed and copied. Chelsea Manning brought music CDs to work under the pretense of listening to them and copied classified data to them.

Harold Martin allegedly removed 50 terabytes of data on disks, hard drives, and thumb drives.

Screen text: Technology
The more technology advances, the more challenging information protection becomes, in part because storage capacity has increased. Aldrich Ames was found to have four floppy disks containing classified information. When arrested, James Nicholson was carrying two floppies containing classified information. Current technology allows even more data to be accessed and copied. Chelsea Manning brought music CDs to work under the pretense of listening to them and copied classified data to them. Harold Martin allegedly removed 50 terabytes of data on disks, hard drives, and thumb drives.

Chelsea Manning

Screen 5 of 18

Narration: Chelsea Manning, a U.S. Army intelligence analyst, leaked more than 750,000 classified documents to WikiLeaks in 2010.

Manning was court-martialed and convicted in July 2013. Manning was dishonorably discharged from active duty and sentenced to 35 years in prison. The prison sentence was commuted in December 2016 and Manning was freed in May 2017.

Screen text: Chelsea Manning

Chelsea (formerly known as Bradley) Manning, a U.S. Army intelligence analyst, leaked more than 750,000 classified documents to WikiLeaks in 2010. Manning was court-martialed and convicted in July 2013.

Manning was dishonorably discharged from active duty and sentenced to 35 years in prison. The prison sentence was commuted in December 2016 and Manning was freed in May 2017.

"I would come in with music on a CD-RW labelled with something like 'Lady Gaga'...erase the music...then write a compressed split file. No one suspected a thing..."

Daniela Greene

Screen 6 of 18

Narration: Daniela Greene was a contract employee with a Top Secret security clearance, hired for her language skills.

In early 2014, she began working as an FBI translator for the Detroit Field Office helping to investigate a German rapper and Islamic State sympathizer who recruited jihadists on the Internet.

During the probe, she alerted the FBI to several online accounts and phone numbers that the subject was using, such as Skype.

Screen text: Daniela Greene
Daniela Greene was a contract employee with a Top Secret security clearance, hired for her language skills.

In early 2014, she began working as an FBI translator for the Detroit Field Office helping to investigate Denis "Deso Dogg" Cuspert, a German rapper and Islamic State sympathizer who recruited jihadists on the Internet.

During the probe, she alerted the FBI to several online accounts and phone numbers that the subject was using, such as Skype.

Greene Arrested

Screen 7 of 18

Narration: Greene was so attracted to the German–born jihadist that she left her husband in the U.S.

In June 2014, she told her FBI supervisor in Indianapolis that she was traveling to Germany to see her family. She completed the required form and listed "vacation/personal" as the reason for going.

She never went to visit her family. Instead she went to Syria to marry the terrorist she was supposed to be watching.

In August 2014, Greene was arrested by the FBI shortly after returning to the U.S. She pleaded guilty to making false statements involving international terrorism. Greene was sentenced to two years in prison and released August 2016.

Screen text: Daniela Greene

Greene was so attracted to the German–born jihadist that she left her husband in the U.S. In June 2014, she told her FBI supervisor in Indianapolis that she was traveling to Germany to see her family. She completed the required form and listed "vacation/personal" as the reason for going. She never went to visit her family. Instead she went to Syria to marry the terrorist she was supposed to be watching. She lived in Syria for 30 days and wrote several e-mails to an individual in the United States, revealing that she committed a criminal act.

In August 2014, Greene was arrested by the FBI shortly after returning to the U.S. She pleaded guilty to making false statements involving international terrorism. Greene was sentenced to two years in prison and released August 2016.

Harold T. Martin

Screen 8 of 18

Narration: Review the case study of Harold T. Martin, a National Security contractor.
Screen text: Harold T. Martin

Harold T. Martin III, a National Security contractor, was arrested in August 2016, after the FBI raided his house and found an estimated 50 terabytes of electronic files in his home office, car, and shed. Martin allegedly had been stealing and hoarding documents containing highly classified information for more than two decades.

Martin held a Top Secret security clearance despite a record that included drinking problems, a drunken-driving arrest, two divorces, unpaid tax bills, a charge of computer harassment, and posing as a police officer in a traffic dispute. These events should have triggered closer scrutiny. He is awaiting prosecution on charges of "stealing government documents and mishandling classified information."

Technology Indicators Screen

9 of 18

Narration: It can be difficult to identify when an insider is using technology to further his or her agenda. However, there are certain indicators that should raise suspicion: improper use of privileged access; working odd hours without authorization; keeping unauthorized backups; and unauthorized requests for, use of, or removal of technical equipment.

Screen text: Technology Indicators

It can be difficult to identify when an insider is using technology to further his or her agenda. However, there are certain indicators that should raise suspicion.

Technology-Related Indicators

- Improper use of privileged access
- Working odd hours without authorization
- Knowingly bypassing technology-associated security rules/protocols
- Inappropriate copying of classified or proprietary information
- Requests for technical or program access beyond scope of work
- Introduction of unauthorized technical devices into the workplace
- Keeping unauthorized backups
- Unauthorized requests for, use of, or removal of technical equipment
- Hoarding files, data, code, and programs

Social Media

Screen 10 of 18

Narration: Before the advent of the Internet and social media, hostile entities would slowly and methodically gather information on personnel through media, travel, social and professional organizations, and public events.

In the social media age, more people share details of their personal and professional lives online, making them much more vulnerable to adversaries.

Screen text: Technology

Before the advent of the Internet and social media, hostile entities would slowly and methodically gather information on personnel through media, travel, social and professional organizations, and public events. It could take years to acquire this information.

Today, we sometimes do that work for them in the space of a weekend on social media. In the social media age, more people share details of their personal and professional lives online, making them much more vulnerable to adversaries, competitors, and cyber-criminals, who all use the Internet as a key targeting tool.

Social Network

Screen 11 of 18

Narration: Although information shared on social network services may not be classified or proprietary, the information can be used to assist adversaries in creating a robust profile of you.

Try to limit what friends, family, and colleagues share about you on social media.

Screen text: Social Media

Although information shared on social network services may not be classified or proprietary, the information can be used to assist adversaries in creating a robust profile of you.

Try to limit what friends, family, and colleagues share about you on social media services.

Privacy Settings

Screen 12 of 18

Narration: Changing your privacy settings is a big step towards limiting who can see your information.

Most social media services allow you to limit who can see details of your profile for each setting option, like this example from Facebook.

Screen text: Privacy Settings

Changing your privacy settings is a big step towards limiting who can see your information.

Countermeasures

Screen 13 of 18

Narration: While many organizations have countermeasures in place to help mitigate the technology-associated insider threat, you play a critical role in helping to protect and safeguard classified or proprietary information.

You can help reduce technology-associated insider threat by: using strong passwords, preventing unauthorized access, and watching for behavioral indicators.

Screen text: Privacy Settings

While many organizations have countermeasures in place (such as auditing, physical security, program access controls, and training) to help mitigate the technology-associated insider threat, you play a critical role in helping to protect and safeguard classified or proprietary information.

You can help reduce technology-associated insider threat by enlisting these countermeasures:

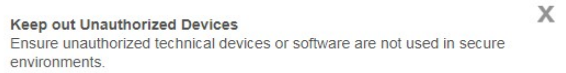
Rollover text boxes:

Use Strong Passwords

Use Strong Passwords

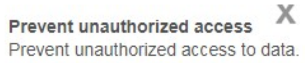
Practice good computer/cyber security by adhering to system protocols, to include using and protecting strong passwords.

Keep out Unauthorized Devices



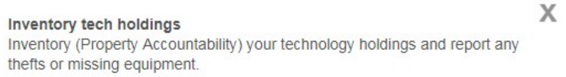
Keep out Unauthorized Devices
Ensure unauthorized technical devices or software are not used in secure environments.

Prevent Unauthorized Access



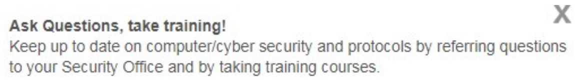
Prevent unauthorized access
Prevent unauthorized access to data.

Inventory Tech Holdings



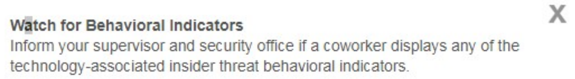
Inventory tech holdings
Inventory (Property Accountability) your technology holdings and report any thefts or missing equipment.

Ask Questions. Take Training!



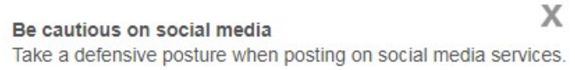
Ask Questions, take training!
Keep up to date on computer/cyber security and protocols by referring questions to your Security Office and by taking training courses.

Watch for Behavioral Indicators



Watch for Behavioral Indicators
Inform your supervisor and security office if a coworker displays any of the technology-associated insider threat behavioral indicators.

Be Cautious on Social Media



Be cautious on social media
Take a defensive posture when posting on social media services.

Knowledge Check 1
Screen 14 of 18

Screen text: Knowledge Check

1. Technological advances impact the insider threat by… ○ Allowing more information to be accessed easily ○ Allowing more information to be transmitted easily ○ Allowing more information to be edited easily ○ All of the above

Knowledge Check 2
Screen 15 of 18

Screen text: Knowledge Check

2. Which of the following is a technology indicator of an insider threat?
   ○ Listening to music services on the Internet ○
   Using Google to search for open source information ○

Hoarding files, data, code, and programs ○ Reading
recent articles in online newspapers

Knowledge Check 3

Screen 16 of 18

Screen text: Knowledge Check

3. How did Manning remove classified documents from a secure facility?
   - ○ Printed them out ○ Stole laptops and hard drives
   - ○ Copied the documents onto a rewriteable music

   CD ○ Saved data on floppy disks

Summary

Screen 17 of 18

Narration: In this lesson, you learned how technological advances impact the insider threat, the vulnerabilities associated with using social media, and about your role in helping to mitigate this threat. In the next lesson, you will learn about reporting requirements.

Lesson Completion

Screen 18 of 18

Narration: Congratulations! You have completed Lesson 4.

Screen text:

Congratulations!
You have completed Lesson 4

LESSON 04 TECHNOLOGY

Lesson 5: Reporting Requirements

Introduction

Screen 1 of 14

Narration: We may be a group of individuals with exceptional talent, dedication, skills, and determination, but we ARE NOT THE EXCEPTION when it comes to being human.

We remain just as vulnerable to insider threats as any other organization in the government or private sector.

We sometimes notice a colleague who is struggling, or a friend who is behaving differently, or a manager bending the rules or acting irresponsibly. We see these things, but far too frequently, do not act on these observations.

Screen text: Lesson 05 Introduction

We may be a group of individuals with exceptional talent, dedication, skills, and determination, but we ARE NOT THE EXCEPTION when it comes to being human. We remain just as vulnerable to insider threats as any other organization in the government or private sector. We sometimes notice a colleague who is struggling, or a friend who is behaving differently, or a manager bending the rules or acting irresponsibly. We see these things, but far too frequently, do not act on these observations.

Reporting Requirements Screen

2 of 14

Narration: Each of us plays a vital role in insider threat mitigation. We have a duty to protect our company's information, our colleagues, and our facilities.

It is our collective responsibility to protect the classified or proprietary information with which we've been entrusted.

Screen text: Reporting Requirements

Each of us plays a vital role in insider threat mitigation. We all have a duty to protect our company's information, our colleagues, and our facilities.

Every member of our workforce should be vigilant, to focus on mission success, but also to keep their eyes and ears open for issues of possible insider threats.

It is our collective responsibility to protect the classified or proprietary information with which we've been entrusted.

Learning Objectives

Screen 3 of 14

Narration: In this lesson you will learn about reporting requirements for insider threat, counterintelligence, and security matters. Review the lesson learning objectives.

Screen text: Reporting Requirements

In this lesson you will learn about reporting requirements for insider threat, counterintelligence, and security matters.

Learning Objectives

After completing this lesson, you will be able to:

- Identify behavioral indicators and activities you should report
- Identify resources for insider threat matters
- Recognize insider threat, counterintelligence, and security reporting requirements

Challenges with Reporting

Screen 4 of 14

Narration: One of the most challenging barriers to reporting insider threat activity is the belief that we are not susceptible.

Screen text: Reporting Requirements

One of the most challenging barriers to reporting insider threat activity is the belief that we are not susceptible.

In a recent survey, respondents expressed concerns about this challenge.

- *"People are naive and complacent, in denial that something could happen now."*
- *"'Talking shop' in public/social settings. Disclosing personal problems, or discussing work-related people, plans and events on-line or in social media (e.g., upcoming trips, promotions, job moves, referencing problems at work, with co-workers or with family etc"*

Report the Information

Screen 5 of 14

Narration: In a previous lesson, you learned about insider threat behavioral indicators. But what, when, and to whom do you report the information?

There is not an all-inclusive list of reportable actions. Let's review terminology to make sure we are all using the same definitions before we discuss reporting requirements.

Screen text: Reporting Requirements

In a previous lesson, you learned about insider threat behavioral indicators. But what, when, and to whom do you report the information?

There is not an all-inclusive list of reportable actions.

Let’s review terminology to make sure we are all using the same definitions before we discuss reporting requirements.

Terms Used

Screen 6 of 14

Narration: Review these terms and their definitions.

Screen text: Reporting Requirements

Terms Used

Contact
Any association, connection, or communication with another individual occurring in person or via any form of technology.

Foreign national
Any person who is not a U.S. citizen or in some instances possesses dual citizenship. Legal permanent residents are foreign nationals.

Personal information
Identifying information which is not commonly known or readily and publicly available such as name, address, or occupation. Information which a foreign national could use to exploit vulnerabilities for CI or security reasons.

Employee Reporting Obligations

Screen 7 of 14

Narration: Personal foreign travel, foreign contacts, and outside activities must be reported.

Screen text: Employee Reporting Obligations & Requirements

- Personal Foreign Travel (even Canada) must be reported
- Personal Foreign Contacts
- Outside Activities (Speeches, Books, Manuscripts)
  - Reportable only if it is going to involve information about activities or involvement with the Intelligence Community.

Employee Reporting Obligations (cont.)

Screen 8 of 14

Narration: Contractors are required to report events that impact the status of the facility, an individual's personnel security clearance, and anything that affects the proper safeguarding of classified information or indications that classified information has been lost or compromised.

Contractors should submit a written report to DCSA and the FBI. A copy of this report will also be provided to the Sponsor.

Contractors shall report efforts by any individual, regardless of nationality to obtain illegal or unauthorized access to classified information or to compromise a cleared employee.

Screen text: Employee Reporting Obligations & Requirements

- Additional Reporting Requirements:
  - Contractors are required to report events that impact the status of the facility, an individual's personnel security clearance, and anything that affects the proper safeguarding of classified/proprietary information or indications that classified/proprietary information has been lost or compromised.
- Reports to be submitted to the FBI:
  - The contractor shall promptly submit a written report to the Defense Security Service and the nearest field office of the FBI regarding information coming to the contractor's attention concerning actual, probable or possible espionage, sabotage, terrorism, or subversive activities at any of their locations.
  - A copy of this report will also be provided to the Sponsor.
- Suspicious Contacts:
  - Contractors shall report efforts by any individual, regardless of nationality to obtain illegal or unauthorized access to classified/proprietary information or to compromise a cleared employee.
  - Any contacts by cleared employees with known or suspected intelligence officers from any country, or any contact which suggests the employee concerned may be the target of an attempted exploitation by the intelligence service of another country.

Reporting Indicators

Screen 9 of 14

Narration: If you witness or experience any of the behavioral indicators we discussed, you must report them to your immediate supervisor and/or your local Security office.

Screen text: Employee Reporting Obligations & Requirements

If you witness or experience any of the behavioral indicators we discussed, you must report them to your immediate supervisor and/or your local Security office. To review, some indicators are:

- Significant changes in personality, behavior, or work habits
- Substance abuse or addictive behaviors (e.g., alcohol and drug abuse/gambling)
- Considerable financial change (e.g., unexplained affluence or excessive debt)
- Disgruntled to the point of wanting to retaliate
- Disregard for security procedures and protocols
- Seeking access to classified or proprietary information and systems/technology without a "need-to-know"
- Access to facilities and/or proprietary information outside of normal work hours
- Unauthorized removal, or unnecessary copying or hoarding of classified or proprietary material

Reportable Activities

Screen 10 of 14

Narration: If you have any knowledge of these activities, report them to your supervisor and local Security office.

Screen text: Reporting Requirements

If you have any knowledge of the following activities, you must report them to your supervisor and local Security office.

- Unauthorized disclosure of classified or proprietary information (spills and/or leaks)
- Improper use of privileged access
- Working odd hours without authorization
- Knowingly bypassing technology-associated security rules/protocols
- Inappropriate copying of classified or proprietary information
- Requests for technical or program access beyond scope of work
- Introduction of unauthorized technical devices into the workplace
- Keeping unauthorized backups
- Unauthorized requests for, use of, or removal of technical equipment
- Hoarding files, data, code, and programs

Assistance & Resources

Screen 11 of 14

Narration: If you or a colleague are experiencing stress, emotional problems, or financial difficulties, do not allow the situation to go unresolved.

There are resources that can help you address the problem such as the EAP. Check your internal organization website for information on how to contact your EAP and find out what services they offer.

Screen text: Assistance & Resources

If you or a colleague are experiencing stress, emotional problems, or financial difficulties, do not allow the situation to go unresolved.

There are resources that can help you address the problem.

Employee Assistance Programs (EAP)

Employees and supervisors are encouraged to call at the first sign of a developing problem. Early assistance can prevent readily solvable problems from developing into major issues. Check your internal organization website for information on how to contact your EAP and find out what services they offer.

Knowledge Check 1

Screen 12 of 14

Screen text: Knowledge Check

1. Which of the following behavioral indicators would you report to your Security office?
    - Disregard for security procedures and protocols
    - Seeking access to classified or proprietary information and systems/technology without a "need to know"
    - Access to facilities and/or proprietary information outside of normal work hours o All of the above

Summary

Screen 13 of 14

Narration: In this lesson, you learned about what you should report related to insider threat.

Screen text: Summary

In this lesson, you learned about what you should report related to insider threat.

Lesson Completion

Screen 14 of 14

Narration: Congratulations! You have completed Lesson 5.

Screen text:

Congratulations!
You have completed Lesson 5

LESSON 05 REPORTING REQUIREMENTS

Conclusion

Screen 1 of 3

Narration: History has taught us that there will always be those who are willing to compromise secrets, whatever their motivation.

No matter how they justify their actions, no individual has the right to decide what classified, sensitive, or proprietary information should be disclosed to another entity, nation, or the public.

Screen text: Conclusion

History has taught us that there will always be those who are willing to compromise secrets.

No individual has the right to decide what classified, sensitive, or proprietary information should be disclosed to another entity, nation, or the public.

Course Conclusion

Screen 2 of 3

Narration: Congratulations! You completed the Insider Threat Awareness course.

Screen text: Conclusion

INSIDER THREAT

Course Exam

Screen 3 of 3

To receive course credit, you must take the course examination. Select the Take Exam button to launch the online exam.

Answer Key

Insider Threat Categories

Knowledge Check 1

Screen 24 of 28

1. What is the name for the unintentional transfer of classified or proprietary information to unaccredited or unauthorized systems, individuals, applications, or media?
   - o Espionage o Sabotage o Spill o Leak

Answer: Spill

Knowledge Check 2

Screen 25 of 28

2. What Targeted Violence subcategory results in physical or psychological harm to the safety and well-being of an employee? o Leak
   - o Workplace Bullying/Violence
   - o Sabotage o Espionage

Answer: Workplace Bullying/Violence

Knowledge Check 3

Screen 26 of 28

3. What is the name for the intentional, unauthorized disclosure of classified or proprietary information to a person or an organization that does not have a "need-to-know"? o Leak
   - o Workplace Bullying/Violence
   - o Sabotage
   - o Espionage

Answer: Leak

Indicators

Knowledge Check 1

Screen 24 of 27

1. Which of the following is NOT an example of a potential insider threat vulnerability?
   - Obesity ○ Drug/alcohol use ○ Loneliness ○ Promiscuity

Answer: Obesity

Knowledge Check 2

Screen 25 of 27

2. Which of the following are examples of behavioral indicators associated with insider threat?
   - Significant changes in personality, behavior, or work habits ○

   Disregard for security procedures and protocols

   - Access to facilities and/or proprietary information outside of

   normal work hours ○ All of the above

Answer: All of the above

Adversaries

Knowledge Check 1

Screen 15 of 19

1. True or False? Adversaries only target you if you have a security clearance.
   - True ○ False

Answer: False

Knowledge Check 2 Screen

16 of 19

2. True or False? You Adversaries only target you if you have a security clearance.
   - True ○ False Answer: False

Knowledge Check 3

Screen 17 of 19

3. Which of the following is NOT a way to deflect an elicitation attempt?

- Ignoring any questions or statements you think are improper and changing the topic ○ Tell them what they want to know up front ○ Stating that you do not know
- Deflecting a question with one of your own

Answer: False

Technology

Knowledge Check 1
Screen 14 of 18

1. Technological advances impact the insider threat by… ○ Allowing more information to be accessed easily ○ Allowing more information to be transmitted easily ○ Allowing more information to be edited easily ○ All of the above

Answer: All of the above

Knowledge Check 2
Screen 15 of 18

2. Which of the following is a technology indicator of an insider threat?
   ○ Listening to music services on the Internet ○ Using Google to search for open source information ○ Hoarding files, data, code, and programs ○ Reading recent articles in online newspapers

Answer: Hoarding files, data, code, and programs

Knowledge Check 3
Screen 16 of 18

3. How did Manning remove classified documents from a secure facility?
   ○ Printed them out ○ Stole laptops and hard drives
   ○ Copied the documents onto a rewriteable music CD ○ Saved data on floppy disks

Answer: Copied the documents onto a rewritable music CD

Reporting Requirements

Knowledge Check 1

Screen 12 of 14

1. Which of the following behavioral indicators would you report to your Security office?
   - ○ Disregard for security procedures and protocols
   - ○ Seeking access to classified or proprietary information and systems/technology without a "need to know"
   - ○ Access to facilities and/or proprietary information outside of normal work hours ○ All of the above

Answer: All of the above