Insider Threat Awareness
Student Guide

February 2024

Center for Development of Security Excellence

Contents

Lesson 1: Course Introduction

Introduction

Welcome

[Video clip, Vigilance series narrator:] Many people believe that insider threat programs are designed to catch bad guys or spy on employees. In reality, these programs are designed to deter, detect, and mitigate risk. Insider threat programs work with a multidisciplinary team of professionals, including security, Human Resources, cyber security, mental health, legal, law enforcement and counterintelligence to identify and evaluate potentially anomalous behaviors that may indicate increased risk and recommend appropriate responses.

The goal of the program is to deter threats and detect potential issues early on before a problem occurs. To be sure, the risk posed by trusted insiders is real and substantial. From compromise of classified information to devastating events resulting in loss of life, insider threats can have a profound impact on national security. However, by working together and recognizing the signs insider threat, programs can often prevent these activities by providing help and support to employees in need, facilitating enhanced security and other countermeasures, and swiftly reacting to threatening situations. We all contribute to the ability of our insider threat programs to find solutions that support national security while protecting individual privacy and civil liberties.

How can you help?

[Course narrator:] It is up to all of us to be aware of potential signs and report what we see. You are your organization's first line of defense against someone who could do harm. On November 5, 2009, Army psychiatrist Major Nidal Hasan opened fired at Fort Hood, killing 13 people and injuring 30 others. Hasan exhibited signs of radicalization for years. On September 16, 2013, Aaron Alexis walked into the Washington Navy Yard with a shotgun, killing 12 people and injuring 3 others. Alexis was a former Navy reservist with a history of mental health problems. These cases influenced the formation of insider threat policy.

This course will familiarize you with insider threat and provide guidance on what to do if you suspect that something is not right.

Objectives

Welcome to the Insider Threat Awareness course. This course focuses on insider threat vulnerabilities, potential behaviors of concern, and reporting requirements.

Course objectives:

- Analyze a scenario and determine the vulnerabilities posed by insiders
- Analyze a scenario and recognize concerning behavior
- Analyze a scenario and apply the appropriate reporting procedures

Lesson 2: Insider Threat Vulnerabilities

Introduction

Objectives

[Vigilance Series video clip, video narrator:] Insider attacks are sometimes difficult to detect, especially since the perpetrators can be people we know and trust. Most people who become witting or unwitting insider threats don't enter the workforce with malicious intent, but over time may experience stressors which when combined with their personal predispositions and trigger events can lead them along a critical pathway to betrayal. Insider threat programs can play a strong role in identifying at-risk individuals and helping them off this pathway toward more positive outcomes, but they can't intervene if they are not aware of the problem.

[Course narrator:] This lesson describes the vulnerabilities posed by insiders.

Lesson Objectives

- Given access and intent attributes, classify whether an individual meets the National Insider Threat Task Force (NITTF) definition for insider threat
- Given a scenario, recognize adversarial collection techniques
- Given a description of predispositions, stressors, and behaviors, recognize an individual who may pose an insider risk

Case Studies

Most insider threats do not start out as a threat; rather, they evolve into a threat over time. Consider Major Nidal Hasan and Aaron Alexis. Major Nidal Hasan displayed concerning behaviors before he carried out the 2009 Fort Hood shooting. Aaron Alexis had a history of mental health issues and was involved in several violent incidents before he carried out the 2013 Washington Navy Yard shooting. The pathway to an insider incident is often complex. By recognizing certain risk factors along a critical pathway, we can work to identify potential threats before they escalate.

Definitions

Who is An Insider?

What do we mean by insider? Consider the following. Who is considered an insider?

Select all that apply.

- ☐ Sue, a cleared DOD employee
- ☐ Kim, a contractor supporting a defense contract
- ☐ Raj, a private sector engineer with no USG contracts married to a DOD employee
- ☐ James, a volunteer supporting cleared facilities
- ☐ Carlos, a civilian access control team member at a DOD facility
- ☐ Lisa, a supply chain vendor for the USG
- ☐ Teresa, a civilian sanitation engineer employed at a USG facility

Insider

An insider is any person with authorized access to any United States Government resource to include personnel, facilities, information, equipment, networks, or systems. This may be through employment, a contractual relationship, or volunteer activities. An insider can be anyone with access. So what makes an insider become a threat?

What is an Insider Threat?

[Mishandling video narrator:] Dave's been working on this high-profile project for a while now. He's been putting a lot of extra hours to try to get stuff done. He was already running late yesterday and decided to take some unclassified work home. He grabbed a stack of documents and rushed out the door in order to meet some friends for dinner. When he got home and looked through his papers, he discovered that he accidentally grabbed some program information. It was a one-page document marked SECRET SAR. Because it was so late at night, he didn't know what else to do so he decided to shred the information in order to protect it.

[Course narrator:] Dave didn’t intentionally bring home a classified document. It was an accident. Could this incident indicate an insider threat?

Select the best response.

- ○ Yes
- ○ No

Insider Threat

Insider threats can be intentional or unintentional.

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

As we saw with Dave, not all threats are deliberate acts. Unintentional acts by insiders can pose just as significant a threat. A significant portion of insider threats involve negligent or accidental behaviors. An insider threat can occur when an individual commits a dangerous act for any number of reasons outside of an intent to harm an organization.

What is Not an Insider Threat?

Consider the following scenarios. Which does NOT indicate a potential insider threat?

Select the best response.

- ○ A scientist at a cleared facility accidentally takes home a document marked SECRET.
- ○ An employee takes a photo at their desk and posts it to social media. Documents marked CUI are visible in the background.
- ○ An analyst has concerns about the CONFIDENTIAL information she's been asked to review and makes a protected disclosure.
- ○ None of these. They all may indicate an insider threat.

Whistleblowing

Making a protected disclosure does not indicate an insider threat.

Whistleblowing is the reporting of waste, fraud, abuse, corruption, or dangers to public health and safety to someone who is in the position to rectify the wrongdoing. Employees are protected from employer retaliation via the Whistleblower Protection Act and Security Executive Agent Directive (SEAD) 9: Whistleblower Protection. It is unlawful for your employer to take any action affecting your access to classified information in reprisal for making a protected disclosure. A disclosure is protected if it meets two criteria.

- The disclosure must be based on the belief that wrongdoing has occurred.
- The disclosure must be made to a person or entity that is authorized to receive it.

Organizations have whistleblowing policies on the correct way to report as opposed to releasing the information to the media or an unauthorized source. Releasing information to the media or an unauthorized source is unauthorized disclosure. It is a crime and is not whistleblowing nor applicable to whistleblower protections. Visit the course Resources to access the Whistleblower Protection Policies and FAQ Job Aid and a real life example of a case where actions were illegal and not protected.

Adversaries

Consider This

[Vigilance series, season 1, episode 2:] Rachel is sitting at her computer when she receives a message via social media offering her a job.

[Course narrator:] Rachel just received a message via social media asking her to write articles about travel, wine, and technology. What should she do?

Select the best response.

- ○ Be careful; it's possible she's being targeted.
- ○ Ask how much it pays.

What Do They Want?

Remember, not all insider threats are intentional. It's possible Rachel is being targeted. If she's not careful, an adversary could collect information from her, making her an unwitting insider threat.

Adversaries include foreign governments, terrorist organizations, competitors, and non-state actors. They want to know non-public information that an insider can provide. This includes information related to:

- Personnel
- Methodologies, capabilities, and limitations
- Facility locations worldwide
- The countries the organization works with

Being aware of what adversaries want helps you protect your organization's information.

Consider This

Consider the following scenarios. Which, if any, may indicate a threat?

Select all that apply.

- ☐ Your company's sales department receives a purchase request from an unknown vendor.
- ☐ A scientist at your facility receives a request to review a research paper.
- ☐ During a conference overseas, a researcher's laptop is stolen.
- ☐ As you arrive at your building early one morning, you encounter a coworker leaving the building. The coworker nervously explains that he sometimes prefers to work overnight.
- ☐ Your organization's network service is disrupted following a denial of service attack.

Collection Methods

Any of these scenarios might point toward a possible threat.

Examining past cases reveals that adversaries commonly use certain collection methods. Understanding these methods can help you identify the presence of a threat. The most common methods, used in over 80% of cases are:

- Requests for information
- Academic solicitation
- Suspicious network activity
- Foreign visits
- Solicitation and marketing or seeking employment
- Targeting at conferences, conventions, and trade shows
- Elicitation and recruitment

Visit the course Resources to access the Collection Methods and Countermeasures Job Aid.

Requests for Information

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

Examples include, but are not limited to:

- Sales
- Representation
- Response to tenders for technical or business services
- Requests under the guise of price quote or marketing surveys

Academic Solicitation

Attempts to acquire protected information under the guise of academic reasons

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

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

Suspicious Network Activity

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

Examples include, but are not limited to:

- Cyber intrusion
- Viruses
- Malware
- Backdoor attacks
- Acquisition of user names and passwords

Targeting at Conferences, Conventions, and Trade Shows

Attempts to directly link programs and technologies with knowledgeable personnel

Technique:

- Technical experts may receive invitations to share their knowledge
- Experts may be asked about restricted, proprietary, and classified information

Solicitation and Marketing/Seeking Employment

Attempts to place foreign personnel near cleared personnel to collect information and build relationships that may be exploited

May take many forms including:

- Joint ventures or research partnerships
- Offering of services
- Internship programs for foreign students

Foreign Visits

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

Examples include, but are not limited to:

- Pre-arranged visits by foreign contingents
- Unannounced visits

Elicitation and Recruitment

Attempts to discreetly gather information that is not readily available and do so without raising suspicion that specific facts are being sought. It is usually non-threatening, easy to disguise, deniable, and effective.

Examples include:

- Conversations in person, over the phone, or in writing
- Commonly occur via social media

Threat Categories

Insider threat categories include:

- Unauthorized disclosure, which can be in the form of a leak – an intentional, unauthorized disclosure of classified or proprietary information to a person or organization that doesn't have a "need-to-know." Unauthorized disclosure can also be unintentional. A spill is the unintentional transfer of classified or proprietary information to unaccredited or unauthorized systems, individuals, applications, or media.
- Espionage is the unauthorized transmittal of classified or proprietary information to a competitor, foreign nation, or entity with the intent to harm.
- Sabotage is the act of deliberately destroying, damaging, or obstructing. While sabotage is often conducted for political or military advantage, personal disgruntlement may also be a motivation.
- Targeted violence is violence directed at an individual or group for a specific reason. It includes everything from active shooter to harassment to workplace bullying.

While you should be aware of the various types of insider threats, know that you likely will not know the intention of a potential threat. Your role is to simply report concerning behavior. Visit the course Resources to access case studies with real life examples of unauthorized disclosure, espionage, targeted violence, and sabotage.

Insider Risk

Consider This

[Vigilance video series clip:]

Tim: I'm definitely interested. I think I can work that out and get it to you as soon as possible. Thank you.

Susan: Hey Tim - working late again?

Tim: Hey Susan – yeah, just finished up a few things. You working late?

Susan: No, I forgot my cellphone. Got about halfway home before I realized. Can you believe that? Me without my phone?

Tim: I know, right? Thing's like your third hand. It's pretty late… I better go feed the dog. Guess I lost track of time.

Susan: I guess so... See you tomorrow, Tim.

[Course narrator:] That was an odd encounter. Susan senses that something isn't right. What should she do?

Select the best response.

- ○ Susan should mind her own business, get her cellphone, and go home.
- ○ Susan should run after Tim and ask him what's wrong.
- ○ Susan should call her coworker and ask their opinion.
- ○ Susan should talk to her supervisor about it.

Who May Pose an Insider Threat?

Susan should talk to her supervisor. Maybe Tim was just working late and maybe he needed to rush home to feed his dog. It isn't Susan's job to know the full picture, and she shouldn't speculate. However, it is her responsibility to report concerning behavior.

There is no one type of person nor single set of circumstances that facilitates an insider act. However, there are certain predispositions and stressors that may signal that an insider may be at increased risk of committing a hostile act. These may make an insider more likely to act on opportunity enabled by their access. It also may make them more susceptible to targeting or exploitation. Without intervention, concerning behavior may escalate, causing potential damage to national security, personnel, facilities, or other resources.

Personal Predisposition

Predisposition refers to an individual's personal characteristics and circumstances that make them more likely to engage in certain behavior. For example, looking at past insider threat cases shows that individuals with a medical or psychiatric disorder or personality or social skills issues are more

likely to engage in risky behavior. Previous rule violations and social network risks are also known predispositions of those who may pose an insider threat.

Going back to the cases of Nidal Hasan and Aaron Alexis, there were several potential predisposing factors that may have contributed to each of their decisions to carry out their attacks. Hasan reportedly expressed radical and extremist beliefs, including support for violent acts. He expressed dissatisfaction with his deployment to Iraq and was reportedly harassed by coworkers for his faith. Alexis reportedly had a history of mental health issues, including paranoid delusions and hearing voices. He also had a prior arrest for discharging a firearm in public. While the specific predisposing factors are different, they may have made them more susceptible to carrying out a violent act.

Stressors

Another risk factor that may contribute to insider threat is stressors. These are events or situations that cause an individual to feel pressure or anxiety and may lead them to act out in ways they normally wouldn't. Common stressors include personal, professional, or financial problems.

In the cases of Nidal Hasan and Aaron Alexis, each experienced several stressors. Hasan reportedly expressed dissatisfaction with his job and was disciplined for performance issues. He also faced personal stressors and reportedly was in the process of getting divorced. Alexis reportedly had significant debts. He also reported feeling isolated and unsupported by his colleagues. These stressors may have made each more susceptible to carrying out their attacks.

Concerning Behavior

Finally, concerning behavior is a potential insider threat indicator. Concerning behaviors are observable behaviors or actions that suggest an individual may be planning or carrying out a malicious act. Concerning behaviors can be categorized by interpersonal behaviors such as arguments or altercations, technical behaviors such as conducting unauthorized computer searches, security behaviors such as failing to follow procedures, and financial behaviors such as unexplained large purchases.

Both Hasan and Alexis displayed concerning behaviors that may have indicated their intentions. Prior to the attack on Fort Hood, Hasan communicated with an operative from a terrorist organization. He researched ways to kill large numbers of people. He also displayed erratic behavior, such as giving away his possessions and preparing his apartment for his departure. Aaron Alexis also displayed several concerning behaviors before carrying out the attack on the Navy Yard. He complained he was being followed by people who were sending vibrations into his body. He was involved in altercations with several people. Two days before the attack, he practiced shooting at a gun range. Taken together, the concerning behaviors of both Hasan and Alexis suggest they were each experiencing significant issues and were exhibiting signs of increased risk for potential violence.

Problematic Organizational Response

Finally, problematic organizational response is a potential insider threat indicator. Inadequate organizational responses can escalate the actions of at-risk employees who are more likely to plan and execute attacks. Examples of problematic organizational responses include inattention, not

having a risk assessment process, inadequate investigation, and other actions that escalate risk. For example, in studying past insider threat cases, in many cases there was insufficient concern prior to the incident. In addition, there was not an organizational mechanism to organize and communicate potential threat information to the appropriate security officials to prevent, deter, detect, or mitigate malicious actions.

The cases of both Hasan and Alexis were integral to establishing policies to develop Insider Threat Programs and guidelines for information sharing between organizations and program pillars. These policies are essential to protect classified information and strengthen national security.

Consider This

[Vigilance video series clip:]

Montenegro: Sorry to hear about you and Sarah splitting and calling off the engagement. That's tough.

Tim: Yeah, but hey…this sure is helping. (Shows Montenegro a picture of his new sports car.)

Montenegro: Whoa, man. That is awesome. Let me see?

Tim: Just picked it up yesterday.

Montenegro: Wow, this is a big step up from your Corolla, bro. That must have set you back a couple bucks.

Tim: Yeah, well…I was shopping for a new car and I figured, why not?

Montenegro: Yeah man, if I came home with something like that, my wife would kill me! You'd be visiting me in the hospital, brother.

Tim: Hey man, you only live once. Sometimes you got to do what you got to do. Listen, I was thinking I'll probably give my two weeks' notice today.

Montenegro: Really? What's going on?

Tim: You know I didn't get the lead programmer position I wanted, right?

Montenegro: Yeah, I heard. That sucks, you should have gotten it.

Tim: I worked my butt off for that job and I really, really needed the money. But it's all good. I figured I might move across the country, Seattle maybe. Be nice to get a road trip with the new wheels…some fresh air.

Montenegro: Wow, are you serious? I mean, there's bound to be other opportunities around here. I mean…hey listen, if this is about Sara, there's plenty of other fish in the sea. You know we'll miss you around here, but hey – Seattle? A road trip in a car like that? All sounds pretty good.

Tim: Montenegro, do me a solid don't talk to anyone about this yet because a chance to talk it over with HR first. Thanks.

[Course narrator:] What potential risk indicators did Major Montenegro see in Tim's behavior?

Select all that apply.

- ☐ Personal issues: His engagement was called off.
- ☐ Professional issues: He didn't get the promotion he wanted.
- ☐ Financial issues: He purchased sports car.
- ☐ None; he just has a lot going on in his life.

Debrief

While there may be a logical explanation, Tim is displaying indicators of personal, professional, and financial issues that could indicate an insider threat.

[Vigilance Series video clip, video narrator:] Major Montenegro is a good friend to Tim. Despite Tim's excitement over his new car, he was able to pick up on some obvious stress and dissatisfaction in Tim's life. While this is nothing unusual, we're all human - it's important to note that many of these normal stressors can lead to negative consequences if not resolved. Reporting this information to a supervisor, human resources, or directly to the insider threat program is a great way to ensure that Tim's situation is evaluated fairly and quickly - whether Tim poses a threat, is at increased risk for targeting or recruitment by an adversary, or simply needs a little help to work through a difficult time. The insider threat program can find a solution that manages insider risk, maintains Tim's privacy, and protects national security.

Conclusion

Summary

You have completed the Insider Threat Vulnerabilities lesson.

Lesson 3: Insider Threat Indicators and Concerning Behavior

Introduction

Objectives

[Vigilance series narrator:] Insider threats come in many forms including sabotage, fraud, theft, workplace violence, unauthorized disclosure, and compromises of classified information. The compromise of classified information can be unintentional - the result of careless security practices or an intentional act perpetrated by an individual working alone or on behalf of an adversary.

Foreign intelligence entities are known to target and recruit trusted insiders as a means of collecting protected data. In addition, many insiders unwittingly place classified information at risk by sharing it with individuals without a need to know. Attempting to access or collect information without authorization is a reportable potential risk indicator of insider threat. Would you recognize it if you saw it? Would you know what to do?

[Course narrator:] This lesson describes insider threat indicators and concerning behaviors.

Lesson Objectives

- Given a scenario, identify reportable behavior indicators
- Given a scenario, recognize the role of Employee Assistance Programs in mitigating potential threat

Case Studies

Insider threats do not need to hold a high rank or position to inflict grave damage. This is in part due to technology that empowers individuals at all levels. Today it is possible for one person, regardless of rank or position in the organization, to do a lot of damage.

Jonathon Toebbe, a U.S. Navy engineer, was sentenced to 18 years for attempting to use his access to sell sensitive nuclear submarine secrets. Harold Martin III, a defense contractor, was sentenced to 9 years for stealing 50 terabytes of classified information. Christopher Paul Hasson, a former U.S. Coast Guard officer, was sentenced to more than 13 years for federal weapons and drug crimes related to plotting violent attacks.

The pathway to an insider incident is often complex. By recognizing insider threat indicators and concerning behaviors, we can work to identify potential threats before they escalate.

To learn more, visit the course Resources to access case studies about Toebbe, Martin, and Hasson.

Risk Indicators

Consider This

[Clip from Vigilance video series, season 1, episode 3:]

Joyce: That's it! See you next week.

Phyllis: The new milestones on this project are impossible!

Joyce: I know, right? After this project is finished, I'm gonna need a long holiday weekend on a tropical beach with some tropical sun and some tropical drinks.

Stewart: I need that travel agent!

Phyllis: Yeah well, I don't think anyone's going on holiday for a while. My problem is I still don't have access to the files on the server like your team does. It would make my life a whole lot easier. I know if I just had some pieces of the source code I need, I could easily make my review date.

Joyce: You're probably right, but you need to talk to Mark about that, Phyllis. A couple weeks ago, I needed some extra information for an article I was publishing in a defense journal. Since he was my supervisor, he hooked me up.

Phyllis: I tried. He doesn't understand. I don't think he ever sees the big picture. I mean, we're all on the same team, right?

Joyce: As far as I know.

Phyllis: Well, if you could do anything to help me out, I'd really appreciate it.

[Transitions to Phyllis alone in the break room, Stewart overhears her on the phone.]

Phyllis: Yes, okay tomorrow sounds fine. Same flight as last time. Yes, I had plenty of time in London to connect to Cyprus. No, thank you. I have someone picking me up.

[Course narrator:] Do you think Phyllis exhibits any potential risk indicators?

Select the best response.

- ○ No; it looks like she’s just trying to do her job.
- ○ Yes; she has a lot going on and her behavior is concerning.

Risk Categories

Phyllis exhibits potential risk indicators. While it's not your responsibility to know specifically what is going on, you do need to recognize potential risk indicators.

Christopher Hasson, a former U.S. Coast Guard officer, is a real-life insider threat whose arrest possibly prevented acts of violence. He was found guilty of federal weapons and drug crimes. Hasson's position in the Coast Guard gave him access to information and facilities. Hasson held extremist views and used his government computer to research violent attacks, including the Unabomber's attacks and manifesto. In addition, Hasson stockpiled assault weapons and opioids.

Risk looks different across organizations. In addition to these categories, risk can generally be delineated as:

- Financial considerations
- Foreign considerations
- Professional performance
- Psychological conditions
- Security or compliance issues

Access Attributes

Include, but are not limited to:

- Security clearance and information access
- Access to physical facilities
- Access to systems and applications
- DOD system(s) privileged user
- Explosives access or training

Violent Extremist Mobilization

Includes, but is not limited to:

- Engaging in or conspiring to engage in violent extremist activities
- Communicating with foreign terrorist organization
- Conducting an attack
- Traveling overseas to join a foreign terrorist organization

Technical Activity

Includes, but is not limited to:

- Violating information system policies
- Suspicious email or browsing activity
- Transferring data to personal or suspicious account
- Tampering with record-keeping data
- Introducing malicious code

Criminal/Violent Conduct

Includes, but is not limited to:

- Exhibiting or threatening violence
- Weapon mishandling
- Failure to follow court order
- Parole or probation violation
- Criminal affiliations
- Suicidal ideation or attempt

Substance Abuse

Include, but are not limited to:

- Illegal substance use or trafficking
- Legal substance abuse or trafficking
- Treatment for abuse of drugs, alcohol, or controlled substances

Financial Considerations

Include, but are not limited to:

- Financial crime
- Filing for bankruptcy
- Delinquent debts
- High debt-to-income ratio
- Failure to file tax returns
- Displaying signs of unexplained affluence
- Gambling problem

Foreign Considerations

Include, but are not limited to:

- Citizenship
- Foreign travel to countries of concern
- Frequent foreign travel excluding official travel
- Foreign military or government service
- Possessing foreign passport
- Possession of foreign assets
- Unauthorized contact with a foreign intelligence entity (FIE)

Professional Performance

Includes, but is not limited to:

- Declining performance ratings
- Poor performance
- Reprimand/non-judicial punishment
- Human Resources (HR) complaints
- Demotion
- Suspension
- Negative characterization of previous employment or service

Psychological Conditions

Include, but are not limited to:

- Anti-social or compulsive behavior
- Communicating endorsement of workplace violence
- Mental instability
- Admission to inpatient mental health facility
- Past untruthfulness

Security/Compliance Incidents

Include, but are not limited to:

- Compliance violation
- Security infraction

- Security violation
- Non-compliance with training requirements
- Time entry violations
- Security clearance denial, suspension, or revocation

Consider This

[Clip from Vigilance series, season 2, episode 2:]

Trish: Hey, Rachel.

Rachel: Oh hi, Trish.

Trish: Some of us are going across the street for some drinks. Come join us!

Rachel: Oh, I'd love to but I'm still trying to finish some work here. With all those contractors leaving, it's like a ghost town over there.

Trish: How did you get approved for overtime?

Rachel: (Grimaces) I didn't, but I still have some work to finish. It's okay, I'll just be a few minutes. Go on, I'll meet you over there.

Trish: All righty.

Rachel: Oh hey, Trish? Can you do me a favor? You're the weapons systems analyst, yes? Could you get me the most recent tech files? You know, please? There could be something in there. I know they're rough drafts, but there may be something in there that could help me finish my own work and then we can all move on.

Trish: Rachel, I've already locked my files for the day…but I guess I can check with my supervisor tomorrow.

Rachel: Never mind, it's okay. I'll just keep slogging on here. Thanks anyway.

(Trish walks away.)

Rachel (talking to herself): CRAP!

[Course narrator:] Did you notice any potential risk indicators?

Select all that apply.

- ☐ Trish asking Rachel to meet the team for drinks.
- ☐ Trish not helping Rachel by sharing her files.
- ☐ Rachel asking Trish for access to her files.
- ☐ Rachel working outside of normal business hours.

Reportable Behavior Indicators

Changing work habits and seeking access to classified information without a "need-to-know" are both reportable behavior indicators.

Jonathan Toebbe is a real-life insider threat who attempted to sell restricted data. He went to great lengths to avoid detection, but ultimately was unable to hide his activities. He smuggled restricted data past security checkpoints a few pages at time over several years – violating security procedures and protocols and, certainly, committing unauthorized removal. He was paid $100,000 in cryptocurrency by FBI agents posing as conspirators.

In addition to these indicators, many known insider threats have been associated with one or more of the following reportable indicators of concerning behavior -

- Significant changes in personality, behavior, or work habits
- Substance abuse or addictive behaviors
- Disgruntled to the point of wanting to retaliate
- Access to facilities and/or proprietary information outside of normal work hours
- Seeking classified or proprietary information, systems, or technology without a "need-to-know"

For covered individuals requiring national security eligibility, these behaviors are tied to the adjudicative guidelines and are required to be reported.

Term	Supplemental Material
Adjudicative Guidelines	Guideline A: Allegiance to the United States Guideline B: Foreign Influence Guideline C: Foreign Preference Guideline D: Sexual Behavior Guideline E: Personal Conduct Guideline F: Financial Considerations Guideline G: Alcohol Consumption Guideline H: Drug Involvement and Substance Misuse Guideline I: Psychological Conditions Guideline J: Criminal Conduct Guideline K: Handling Protected Information Guideline L: Outside Activities Guideline M: Use of Information Technology

Consider This

[Clip from Vigilance video series, season 1, episode 3:]

[No dialog - Stewart observes Phyllis looking over Joyce's shoulder at Joyce's computer screen.]

Stewart: I'm going to the breakroom.

[No dialog - Stewart observes Phyllis removing a thumb drive from a computer.]

[Course Narrator:] Now what is Phyllis up to?

Does Phyllis exhibit any potentially concerning behavior?

Select all that apply.

- ☐ Looking at her co-worker's computer over her shoulder
- ☐ Not going to the break room when Stewart said he was going
- ☐ Using a flash drive
- ☐ Being in a bad mood and not being a team player

Technology-Related Indicators

There may be a logical explanation, but Phyllis' behavior is concerning. Remember, it is your responsibility to be aware of concerning behavior. It is not up to you to speculate if it may indicate an actual threat.

Real-life insider threat Harold Martin III used his position as a contractor to steal terabytes of classified data over 30 years. Clearly, he must have displayed some concerning behavior over that time. Improper use of privileged access, hoarding, and knowingly bypassing protocols are all reportable technology-related behaviors.

Many known insider threats have been associated with one or more of these and the following technology-related indicators:

- Working odd hours without authorization
- 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

Getting Help

Consider This

[Clip from Vigilance series, season 2, episode 2:]

News broadcast: In other news from Washington, the federal government has announced a new round of budget cuts that could impact a number of government agencies.

Government supervisor: There'll be no more overtime for federal employees and no performance bonuses until further notice.

Carmen: Our contract ends in two months. I'm sorry to have to tell you that we have received official government notification that it will not be renewed.

Antonio (talking to himself at his desk): I've only found two job possibilities in three weeks and neither of them come close to paying me what I was making here. I just hope and pray we don't have to sell the house and move and start all over again.

Carmen: Good morning, Antonio.

Antonio: What's up?

Carmen: Well, I was wondering where you were this morning.

Antonio: What do you mean? I was here at my desk!

Carmen: Well, you weren't at the Monday team meeting again.

Antonio: Huh, oh yeah. Guess I forgot. Anyway, I don't know what difference it makes at this point. I mean, why bother?

Carmen: Well, we still have to finish as much of the final schematics as we can and a rough outline for going forward.

Antonio: Going forward? For what?! To unemployment?! I mean, to be honest with you, Carmen… if I had any more sick leave or paid time off I'd just take it, but I guess I could work on it a bit more.

Carmen: We're all bummed about this, but we still have to as much as we…

Antonio: Hey, I said I would work on it, okay?!

[Course narrator:] That didn't go very well. Antonio is clearly stressed. What should Carmen do?

Select the best response.

- ○ She should mind her own business; he's just having a bad day.
- ○ He's clearly having a hard time. She should get him some help.
- ○ Even though the contract is almost up, she should fire Antonio.

Employee Assistance Programs

Yes, Antonio might need some extra help.

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. The Employee Assistance Program (EAP) is designed to help employees navigate these issues. 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.

Debrief

[Vigilance series clip, narrator:] People who exhibit concerning behaviors are not always bad people. They may not necessarily be doing something wrong. Sometimes stressors build up over time and that can lead to troubling behavior. Most insider threats exhibit risky behavior prior to committing negative workplace events.

Conclusion

Summary

You have completed the Insider Threat Indicators and Concerning Behaviors lesson.

Lesson 4: Reporting Requirements

Introduction

Objectives

[Vigilance Series Video Narrator:] Co-workers, supervisors, and managers are often the first to sense that an individual is experiencing stress or personal issues. Many of us may be hesitant to report this information. After all, everyone has stressful life experiences or has a bad day occasionally. No one wants to cause trouble for a friend or co-worker or be thought of as crying wolf over nothing.

Consider though that insider threat programs are multidisciplinary in nature and designed to evaluate the entirety of the situation and can often put reported indicators in context. They treat each matter individually with utmost respect for privacy and civil liberties. Mitigation response options often include solutions that provide help and resources for those in need. We all have a duty to report indicators. Being nervous about it is natural but consider the consequences of not reporting. How can you help your fellow employees while fulfilling your security responsibilities?

[Course narrator:] This lesson describes insider threat reporting procedures.

Lesson Objectives

- Given a scenario, recognize the role all employees play in ensuring an organization's security
- Given a scenario, identify to whom to report concerning behavior

Reporting Concerning Behavior

Roles and Responsibilities

[Clip from Vigilance series, Season 2, Episode 3 Video narrator:] Reporting can be difficult for employees, but coworkers are right to do so. Employees of cleared industry and federal agencies must report potential threats. Early reporting allows insider threat programs to pursue a multidisciplinary approach to gathering and reviewing information.

[Course narrator:] Security is the responsibility of everyone in an organization. Employees are the first line of defense against insider threats and are responsible for reporting concerning behavior. While all employees are responsible for reporting concerning behavior, organizations also have specific teams and individual roles in place to protect against insider threats.

- The Insider Threat Program addresses and analyzes information from multiple sources regarding concerning behaviors and any risks that could potentially harm an organization.
- The Insider Threat Program Senior Official implements Insider Threat Program activities, including daily operations, management, and ensuring standards compliance.

- The Facility Security Officer (FSO) is in charge of managing security in their organization's facilities.
- An organization's leadership promotes a protective and supportive culture throughout the organization in support of employees and the organization's Insider Threat Program.

Obligations

Reporting foreign collection attempts is required by both DODD 5240.06 and the National Industrial Security Program Operating Manual (NISPOM). Who you report to depends on if you are a DOD, cleared industry, or federal agency employee.

- DOD employees: Report potential threats to your organization's Insider Threat Program
- Cleared industry employees: Report to the facility Insider Threat Program Senior Official (ITPSO) or Facility Security Officer (FSO)
- Federal agency employees: Report to your agency's Insider Threat Program, security office, or supervisor

Failure to report can result in fines, prison, or both. Specific reporting procedures vary, follow your organization's reporting procedures.

What to Report

If you suspect a possible threat, you must report it. You cannot assume anyone else will do so.

Specifically, all employees must report personal foreign travel (including to Canada), personal foreign contacts, outside activities (speeches, books, manuscripts) involving the Intelligence Community, and efforts by anyone (regardless of nationality) to obtain illegal or unauthorized access to classified or proprietary information or to compromise a cleared employee. Finally, all employees must report contacts by cleared employees with known or suspected intelligence officers from any country, or any contact which suggests the employee may be the target of an attempted exploitation by the intelligence service of another country.

Contractors have additional requirements, and there are specific requirements for reports submitted to the FBI.

Additional Contractor Requirements

Contractors are required to report events that impact:

- The status of the facility
- The status of an individual's personnel security clearance
- Anything that affects the proper safeguarding of classified/proprietary information
- Indications that classified/proprietary information has been lost or compromised

Reports Submitted to the FBI and DCSA

Reports to be submitted to the FBI by the appropriate security official:

- The contractor shall promptly submit a written report to the Defense Counterintelligence and Security Agency and the nearest field office of the FBI regarding information coming to the contractor's attention concerning actual, probable, or possible:
  - Espionage
  - Sabotage
  - Terrorism
  - Subversive activities

Scenarios

Overview

Earlier in this course, you met Tim, Rachel, and Phyllis. Let's review a briefing for each and explore what, if anything, should be reported and to whom.

Rachel:

- Targeted on social media
- Worked late without approval
- Asked coworker for files

Tim:

- Personal stressors
- Professional stressors
- Financial stressors

Phyllis:

- Seeking information without approval
- Unauthorized use of flash drive
- Foreign travel

Rachel: Briefing

Rachel is a federal government employee who was contacted via social media.

Since receiving the first message on social media, Rachel has received more messages asking increasingly detailed questions about her work. What should she do?

Select the best response.

- ○ Answer their questions
- ○ Ignore then sender and block them
- ○ Self-report

Rachel: Feedback

Rachel needs to self-report the contact. People are targeted this way all the time.

In 2018, Henry Kyle Frese was contacted by a journalist via Twitter direct message. He failed to report the journalist's suspicious requests for national defense information. Instead, he accessed information outside the scope of his job duties. For over a year, Frese passed classified information to journalists and a potential romantic partner for personal gain. He was arrested in the fall of 2019 and was sentenced to 30 months in prison for the unauthorized disclosure of classified national defense information to two journalists. To learn more, visit the course Resources to access a case study about Frese.

Rachel: Reporting

Rachel knows she must self-report the unsolicited messages she received via social media. To whom should she report?

Select the best response.

- ○ Report to her organization's Insider Threat Program, security office, or her supervisor.
- ○ Report to the media so they can warn the general public.
- ○ Report to her co-workers and her network provider.

Feedback: *As a Federal employee, Rachel must report to her organization's Insider Threat Program, security officer, or her supervisor. If her co-workers are aware she was contacted, they are also required to report it.*

Tim: Briefing

Tim is a DOD employee. His coworker Maj. Montenegro is concerned about him. Tim is exhibiting several potential risk indicators.

What should Maj. Montenegro do?

Select all that apply.

- ○ Don't report it; it's not his responsibility because it doesn't pose an imminent threat.
- ○ Don't report it; it's not his responsibility because he doesn't think it involves a foreign entity.
- ○ Report it; it's everyone's responsibility to report concerning behavior.

Tim: Feedback

Major Montenegro needs to report the concerning behavior so that it can be evaluated. It's likely Tim just needs some help and to be referred to his organization's Employee Assistance Program. Reporting helps people off a potential critical path to a more positive outcome.

Tim: Reporting

To whom should Maj. Montenegro report Tim's concerning behavior?

Select the best response.

- ○ His supervisor
- ○ His organization's Insider Threat Program
- ○ His security office

Feedback: *DOD reporting procedures state to report to the organization's Insider Threat Program.*

[Vigilance video series clip]

Major Montenegro: Anyway, Marc, I just thought you should know what happened. Tim's a really good guy. I have known him for about three years now. We played softball together. We've gone to some concerts and stuff. He didn't get the lead programming position that he wanted and then he broke up with his fiancée. I know he's had some financial problems and lately he's been working some crazy hours. He's been really down. I really liked him, but I thought I should just report what happened yesterday. Maybe you can cut him some slack?

Marc: Thanks, Major. I know you liked him. In fact, we all do that's why I'm so happy you came in to talk to me today. Tim may be having some problems, but he's still a valued employee that we want to help out during periods of stress or transition. Our agency has so many resources available to folks whether they're struggling personally, professionally, or financially - most people don't even realize that. Anyway, I will work with the insider threat team to assess the situation.

Major Montenegro: Insider threat? Wait a minute, I don't want to get Tim in any trouble.

Marc: The insider threat team isn't there to get anyone in trouble and we work together all the time to improve security practices, increase awareness, and identify employees who may be at risk. Most of the time we're able to resolve issues swiftly. Don't worry. Tim's in good hands and you did the right thing by coming to me. But please, let's keep this between us. I don't want anyone to start rumors about Tim

Major Montenegro: Yes, sir. Thank you.

Phyllis: Briefing

Phyllis is an employee of a cleared defense contractor. Her coworkers have noticed several suspicious behaviors from her.

What concerning behavior should Phyllis' coworkers report?

Select all that apply.

- ☐ Studying her co-worker's computer screen over her shoulder
- ☐ Using a flash drive
- ☐ Asking her coworkers for the source code after the supervisor denied her request
- ☐ Traveling travel to London and Cyprus without self-reporting

Phyllis: Feedback

All of these behaviors are concerning and should be reported by her coworkers.

In the first example, Phyllis is attempting to covertly look at information on her co-worker's computer. Maybe she's just being nosey, but without a need-to-know she shouldn't be looking at all. Anyone observing such behavior is required to report it. Removable storage devices should not be connected to computers within a protected network unless prior approval has been granted. Seeking to work around a supervisor's denial of access to classified information must also be reported. Finally, while there's nothing wrong with traveling out of the country, persons with access to classified information are required to self-report when they plan to travel overseas. Failing to do so must also be reported.

Daniel Hale is a real-life insider threat. He was a DOD contractor who used technology to exfiltrate national defense information. He purposefully disregarded the law and passed classified information to journalists. Hale's disclosure of classified documents resulted in the documents being published and available for public view, to include by adversaries. Their disclosure could cause exceptionally grave damage to the United States. Hale pleaded guilty to retention and transmission of national defense information and was sentenced to 45 months in prison.

To learn more, visit the course Resources to access a case study about Hale.

Phyllis: Reporting

To whom should Phyllis' coworkers report Phyllis' concerning behavior?

Select all that apply.

- ☐ Report to Phyllis' supervisor.
- ☐ Report to the facility Insider Threat Program Senior Official (ITPSO) or Facility Security Officer (FSO).
- ☐ Report directly to the FBI.

Feedback: *The 32 CFR Part 117 NISPOM Rule states that contractors must report to their facility Insider Threat Program Senior Official (ITPSO) or Facility Security Officer (FSO).*

Wrap Up

[Vigilance narrator:] The risk posed by trusted insiders is real and substantial. From compromise of classified information to devastating events resulting in loss of life, insider threats can have a profound impact on national security.

[News announcer:] In Washington today, Applied Technologies confirmed an unauthorized disclosure of information that could compromise the latest US drone avionics program and national security.

[Course narrator:] We are all responsible for security. If you encounter concerning behavior, you must report it.

Conclusion

Summary

You have completed the Reporting Requirements lesson.

Lesson 5: Course Conclusion

Conclusion

Summary

This course familiarized you with insider threat and provided guidance on what to do if you suspect that something is not right. It is up to all of us to be aware of potential signs and report what we see. You are your organization's first line of defense against someone who could do harm.

Conclusion

Congratulations! You have completed the *Insider Threat Awareness* course.

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

- Analyze a scenario and determine the vulnerabilities posed by insiders
- Analyze a scenario and recognize concerning behavior
- Analyze a scenario and apply the appropriate reporting procedures

To receive course credit, you must take the *Insider Threat Awareness* examination. Please use the Security Training, Education, and Professionalization Portal (STEPP) system from the Center for Development of Security Excellence to access for the online exam.