Center for Development of Security Excellence

CDSE

INSIDER THREAT JOB AID

FACILITATION GUIDE

Insider Threat Vigilance Series Episode One: An Odd Encounter With Tim

Overview: The Insider Threat Vigilance Series aids the workforce in understanding how to identify and report insider threat indicators. The series also provides an overview of how Insider Threat Programs (also known as Insider Threat HUBs) take a multi-disciplinary staff approach towards analyzing information and activity indicative of an insider threat and referring that data to the appropriate officials to investigate or otherwise resolve. The goal of the program is to deter threats and detect potential issues early on—before a problem occurs.

This guide will aid you in presenting the video to your training audience. Use the questions below to assist with your group discussion. You can access the episode on YouTube or in a micro-learning module with expanded information and resources.

YouTube Location: https://www.youtube.com/watch?v=Kr2QAdHBMB4&feature=youtu.be

Micro Learn Location: https://www.cdse.edu/micro/vigilance-episode1/vigilance-episode1.html

Instructions

Video Segment 1: Play video and then pause it at 3:30, after the narrator says “What would you do?” Consider asking the students the following questions.

Question 1: What potential risk indicators did Susan see in Tim’s behavior?

Desired Responses:

- Tim was talking on his phone in a muffled voice
- Tim was working late and by himself at the office
- Tim quickly minimized his computer screen and shut down his computer
- Tim placed folders in his briefcase and rushed out of the office and left a sandwich and hot cup of coffee at his desk

Question 2: What Should Susan do?

Desired Response: Report Tim to the Insider Threat Program

Additional Comment: Correct students if they recommend taking matters into their own hands in conducting investigative activity, such as: going through his desk drawers, trying to follow him, questioning other employees about Tim’s behavior, etc.

Video Segment 2: Un-pause the video and watch Susan's interaction with the Insider Threat POC (Beth Sloan).

Question 3: Did Beth take any immediate adverse actions against Tim?

Desired Responses: No, she realized Tim's behavior was suspicious and outside of the norm. However, she does not have enough information to understand why Tim is acting abnormally. Her main concern was understanding what happened and sharing the information with the other members of the Insider Threat Program. By alerting the other Insider Threat Team Members (HR, Cyber, LE, CI, etc.), she may be able to get additional information that sheds light on why Tim is behaving oddly.

She didn't have enough information to warrant suspending a clearance, firing, or reprimanding him in anyway.

Question 4: Was Tim's privacy protected?

Desired Responses: Yes, Beth informed Susan not to tell anyone about Tim's behavior. Beth did not jump to any conclusions or take any overly intrusive actions against Tim.

Susan reported what she observed but **did not** take steps towards conducting an investigation of her own. If Susan would have searched through Tim's desk, followed him, conducted surveillance, or questioned other employees about Tim's behavior, her activities might have been inappropriate, a violation of policy/regulation, and/or potentially illegal.

Question 5: Do you know where and how to report potential threat Indicators?

Possible Discussion: Please take the opportunity to discuss your organization's Insider Threat Program and reporting procedures.

Additional Facilitator Resources

- Insider Threat Toolkit: https://www.cdse.edu/toolkits/insider/index.php\
- Counterintelligence Toolkit: https://www.cdse.edu/toolkits/ci/index.php
- DoD Insider Threat Trifold: https://www.cdse.edu/documents/cdse/DoD_Insider_Threat_Trifold.pdf
- Insider Threat Case Studies: https://www.cdse.edu/resources/case-studies/insider-threat.html
- Security Briefing Templates: https://www.cdse.edu/toolkits/fsos/security-education.html
- Security Posters: https://www.cdse.edu/resources/posters.html
- Potential Espionage Indicators (PEI) Detecting Actions Outside the Norm Webinar (30 minutes): https://www.cdse.edu/catalog/webinars/counterintelligence/potential-espionage-indicators.html
- Adverse Information Reporting Webinar (30 Minutes): https://www.cdse.edu/catalog/webinars/industrial-security/adverse-information-reporting.html
- Preserving Investigative and Operational Viability in Insider Threat Course (60 minutes): https://www.cdse.edu/catalog/elearning/INT220.html

Center for Development of Security Excellence

CDSE

INSIDER THREAT JOB AID

FACILITATION GUIDE

Insider Threat Vigilance Series Episode Two: “Check Out My New Ride”

Overview:

The Insider Threat Vigilance Video Series aids the workforce in identifying and reporting insider threat indicators. The series also provides an overview of Insider Threat Programs and their multi-disciplinary approach to gathering and reviewing information indicative of an insider threat, referring that data as appropriate, and developing mitigation response options all while protecting the privacy and civil liberties of the workforce. The goal of the program is to deter threats and detect potential issues early on—before a problem occurs.

This guide will aid you in presenting the video to your training audience. Use the questions below to assist with your group discussion. You can access the episode on YouTube or in a micro-learning module with expanded information and resources.

YouTube Location: https://youtu.be/E9w9bDyH1rU

Micro-Learning Location: https://www.cdse.edu/micro/vigilance-episode2/vigilance-episode2.html

Instructions

Play the video for your group and consider asking the following questions.

Question 1: What potential risk indicators did MAJ Montenegro see in Tim’s behavior?

Desired Responses:

- Splitting up with his girlfriend and calling off their engagement
- Purchase of expensive car
- Mentioned having financial difficulties
- Put in his two week notice
- Discouraged because he didn’t get the lead programmer position

Question 2: Why could Tim’s behavior be considered suspicious?

Desired Responses:

- Financial Considerations: Tim is discouraged because he didn’t get the promotion. During his conversation with MAJ Montenegro, he said, “I really needed the money.” He then mentioned that he had purchased an expensive car. It’s odd that Tim needed the promotion for “the money” but was then able to purchase an expensive vehicle. Tim also mentioned planning to put in his two week notice and leave his job. Tim's purchase of the vehicle could be an example of unexplained affluence.

- Personal Conduct: Tim split up with his girlfriend, and they have called off their engagement. The ending of a serious relationship is a difficult life situation. When combined with not getting the promotion and possibly having some financial difficulties, Tim could be going through a life crisis. Tim's personal predispositions will determine how he handles the crisis.

Additional Comment: If the group has watched episode 1, "An Odd Encounter with Tim," you may ask them to discuss some of the potential risk indicators he displayed in episode 1.

- Tim was talking on his phone in a muffled voice
- Tim was working late and by himself at the office
- Tim quickly minimized his computer screen and shut down his computer
- Tim placed folders in his briefcase and rushed out of the office and left a sandwich and hot cup of coffee at his desk

In episode 1, Tim displayed some suspicious personal conduct. Mark Smith and MAJ Montenegro were probably unaware of Tim's previous suspicious behavior reported by Susan in episode 1. In this episode, Tim displays some potentially risky financial indicators and personal conduct. MAJ Montenegro and Mark Smith's reporting will help the Insider Threat Program gain additional context on Tim's situation.

Question 3: What did MAJ Montenegro do?

Desired Response: MAJ Montenegro was concerned about Tim's behavior. He decided to discuss his concerns with Tim's supervisor, Mark Smith. Mark was also concerned about Tim's behavior and decided to contact the organization's Insider Threat Program.

Question 4: What is an Insider Threat Program?

- Designed to identify "at risk" individuals and help them off this pathway and toward more positive outcomes.
- Insider Threat Programs often assist with solutions that focus on providing help and resources for those in need.
- Insider Threat Programs are multidisciplinary. They typically include representatives from CI, Law Enforcement, Cyber, behavioral health, and legal. As a team, the group can look at Tim's situation and best determine how to mitigate risk to the organization – including options that would help Tim onto the right path.

Additional Comment: This is a good point to ask the group if they know how to report information to their Insider Threat Program. The facilitator should provide contact information for their organizational Insider Threat Program.

Question 5: Why was it important for MAJ Montenegro and Mark to report Tim's behavior?

Desired Responses: Mark and MAJ Montenegro are concerned about Tim. They didn't jump to any conclusions, but it is possible that Tim is involved in espionage or other criminal or harmful activity. Ultimately, they really don't know what is going on with Tim. They are concerned about Tim's behavior and want to get him help if it is needed.

Insider Threat Programs have access to many resources including the Employee Assistance Program that can help Tim. If Tim is having trouble, the Insider Threat Team wants to get him the help he needs before he becomes an insider threat.

It's possible that other co-workers have concerns about Tim's behavior. Maybe they reported him as well (see episode 1). Mark and the MAJ's reporting could give the Insider Threat Team additional context into Tim's situation. More importantly, what if Mark and the MAJ are the only ones to notice Tim's suspicious behavior, or are the only ones that knew to report it? Mark and MAJ Montenegro could be the Insider Threat Team's only opportunity to know Tim is struggling.

Additional Facilitator Resources

- Insider Threat Toolkit: https://www.cdse.edu/toolkits/insider/index.php
- Counterintelligence Awareness Toolkit: https://www.cdse.edu/toolkits/ci/index.php
- DoD Insider Threat Trifold: https://www.cdse.edu/documents/cdse/DoD_Insider_Threat_Trifold.pdf
- Insider Threat Case Studies: https://www.cdse.edu/resources/case-studies/insider-threat.html
- Customizable DoD Command Briefing: https://www.cdse.edu/documents/cdse/customizable-dod-command-brief-for-insider-threat-awareness.pdf
- Security Posters: https://www.cdse.edu/resources/posters.html
- Potential Espionage Indicators (PEI): Detecting Actions Outside the Norm Webinar (30 minutes):
- https://www.cdse.edu/catalog/webinars/counterintelligence/potential-espionage-indicators.html
- Adverse Information Reporting Webinar (30 Minutes): https://www.cdse.edu/catalog/webinars/industrial-security/adverse-information-reporting.html
- Preserving Investigative and Operational Viability in Insider Threat Course (60 minutes): https://www.cdse.edu/catalog/elearning/INT220.html

Center for Development of Security Excellence

CDSE

INSIDER THREAT JOB AID

FACILITATION GUIDE

Insider Threat Vigilance Series Episode Four: "Meeting of the Minds"

Overview:

The Insider Threat Vigilance Video Series aids the workforce in identifying and reporting insider threat indicators. The series also provides an overview of Insider Threat Programs and their multi-disciplinary approach to gathering and reviewing information indicative of an insider threat, referring that data as appropriate, and developing mitigation response options while protecting the privacy and civil liberties of the workforce. The goal of the program is to deter threats and detect potential issues early on—before a problem occurs.

This guide will aid you in presenting the Insider Threat Vigilance video to your training audience. Use the questions below to assist with your group discussion. You can access the episode on YouTube or in a micro-learning module with expanded information and resources.

YouTube Location: https://youtu.be/RZHQW3d819M

Micro-Learning Location: https://www.cdse.edu/micro/vigilance-episode4/vigilance-episode4.html

Instructions

Play the video for your group and consider asking the following questions:

Question 1: Where might the agency have to report Joyce's unauthorized disclosure?

Desired Responses:

- Department of Defense
- Congress
- Federal Bureau of Investigation

Question 2: What role do each of the agencies mentioned play with respect to unauthorized disclosure? Desired Responses:

- Department of Defense: All serious security incidents involving espionage; unauthorized disclosure to the public media or that is reported to the oversight committees of Congress; special access programs or anything relating to defense operations, systems, or technology likely to cause significant harm or damage to U.S. national security; unauthorized disclosure of Sensitive Compartmented Information (SCI); or egregious security incidents as determined by the DoD Component senior agency official.

- Congressional Oversight Committees: Some authorized disclosures are so serious or of such interest to the public that DoD must report them to Congress. After consulting with the Director of National Intelligence (DNI) and the Director of the Federal Bureau of Investigation (FBI), the Office of the Under Secretary of Defense for Intelligence (OUSD(I)) must report to Congress on behalf of the Secretary of Defense each failure or compromise of classified information that the Secretary of Defense determines is likely to cause damage to national security. The Secretary of Energy must report to Congress each security incident involving unauthorized disclosure of restricted data and/or formerly restricted data.

- Federal Bureau of Investigation: Section 811 of the Intelligence Authorization Action of 1995 (50 US Code 402a) is the legislative act that governs the coordination of counterintelligence investigations between Executive Branch agencies and departments and the FBI. Section 811 referrals are reports that advise the FBI of any information, regardless of origin, that may indicate that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or agent of a foreign power.

Question 3: In addition to the reporting requirement, what other action was mentioned that may occur as a result of the unauthorized disclosure?

Desired Response: Sanctions were mentioned. Those who are responsible for unauthorized disclosure face serious consequences. After the investigation is conducted, commanders and supervisors may consider and impose a wide range of sanctions and actions against those found responsible for unauthorized disclosure of classified information. These consequences can take the form of Uniform Code of Military Justice (UCMJ) sanctions, civil litigation, administrative sanctions, and criminal sanctions. For example, individuals may have their accounts suspended and only reinstated after completion of remedial training.

Additional Discussion: If the group has watched the previous three videos, you may ask them to discuss some of the potential risk indicators displayed in those episodes and discuss what an insider threat program is and why it is important.

Indicators from Previous Episodes:

- Splitting up with his girlfriend and calling off their engagement
- Purchasing an expensive car
- Having mentioned financial difficulties
- Unexpectedly submitting his two week notice
- Discouraged because he did not get the lead programmer position
- Working late, quickly turning off computer screen, and talking quietly to someone on the phone
- Inserting USB thumb drives into systems
- Foreign travel
- Attempts to gain access to information outside of normal scope of duties

Additional Discussion: What is an Insider Threat Program?

- Designed to identify "at risk" individuals and help them off this pathway and toward more positive outcomes.
- Insider Threat Programs often assist with solutions that focus on providing help and resources for those in need.
- Insider Threat Programs are multidisciplinary. They typically include representatives from security, counterintelligence, human resources, law enforcement, cyber, behavioral health, and legal. As a team, the group can look at each situation and best determine how to mitigate risk to the organization, including options that would help get employees onto the right path.

Additional Discussion: This is a good time to ask the group if they know how to report information to their Insider Threat Program. The facilitator should provide contact information for their organizational Insider Threat Program.

Additional Facilitator Resources

- Insider Threat Toolkit: https://www.cdse.edu/toolkits/insider/index.php

- Counterintelligence Awareness Toolkit: https://www.cdse.edu/toolkits/ci/index.php

- DoD Insider Threat Trifold: https://www.cdse.edu/documents/cdse/DoD_Insider_Threat_Trifold.pdf

- Insider Threat Case Studies: https://www.cdse.edu/resources/case-studies/insider-threat.html

- Customizable DoD Command Briefing: https://www.cdse.edu/documents/cdse/customizable-dod-command-brief-for-insider-threat-awareness.pdf

- Security Posters: https://www.cdse.edu/resources/posters.html

- Potential Espionage Indicators (PEI): Detecting Actions Outside the Norm Webinar (30 minutes): https://www.cdse.edu/catalog/webinars/counterintelligence/potential-espionage-indicators.html

- Adverse Information Reporting Webinar (30 Minutes): https://www.cdse.edu/catalog/webinars/industrial-security/adverse-information-reporting.html

- Preserving Investigative and Operational Viability in Insider Threat Course (60 minutes): https://www.cdse.edu/catalog/elearning/INT220.html

- Unauthorized Disclosure: Educate Yourself https://www.cdse.edu/toolkits/unauthorized/educate.html

Center for Development of Security Excellence
CDSE

INSIDER THREAT JOB AID

FACILITATION GUIDE

Insider Threat Vigilance Series Episode Three: "What's Pre-Publication Review?"

Overview:

The Insider Threat Vigilance Video Series aids the workforce in identifying and reporting insider threat indicators. The series also provides an overview of Insider Threat Programs and their multi-disciplinary approach to gathering and reviewing information indicative of an insider threat, referring that data as appropriate, and developing mitigation response options all while protecting the privacy and civil liberties of the workforce. The goal of the program is to deter threats and detect potential issues early on—before a problem occurs.

This guide will aid you in presenting the video to your training audience. Use the questions below to assist with your group discussion. You can access the episode on YouTube or in a micro-learning module with expanded information and resources.

YouTube Location: https://youtu.be/twSKE16nMrY

Micro-Learning Location: https://www.cdse.edu/micro/vigilance-episode3/vigilance-episode3.html

Instructions

Play the video for your group and consider asking the following questions:

Question 1: What suspicious behavior did Stuart see Phyllis displaying?

Desired Responses:

- Looking over coworkers' cubicles while they were working
- Seeking access to information outside her scope of duties
- Inserting a USB device in her computer and placing it in her purse
- Talking quietly on phone about foreign travel

Question 2: Why could Phyllis' behavior be considered suspicious?

Desired Responses:

- Access Attributes and Need to Know: Phyllis' interest in her coworkers' work has led one of her coworkers to take notice. That same coworker sees Phyllis removing a USB device and placing it in her bag. Phyllis then discusses her need for additional access. USB devices present a security risk as they allow the transfer of large amounts of data. Coworkers attempting to gain access to information outside their scope of work is a potential indicator because they may be trying to obtain it for foreign adversaries.

- Foreign Considerations: Phyllis is overheard engaging in a quiet telephone conversation about foreign travel. Foreign locations are often used as venues for meeting places and transferring information. An organization's security office will handle documenting and/or approving foreign travel, particularly if they have a security clearance or access to sensitive information.

Question 3: Why is pre-publication review important?

Desired Response: Pre-publication is required and prevents unauthorized release of information that could be damaging to national security. The Defense Office of Prepublication and Security Review (DOPSR) is responsible for managing the DoD security review program. It reviews materials both for public and controlled release. You may reference DoD Directives 5230.09, Clearance of DoD Information for Public Release, and DoD Instruction 5230.09, Security and Policy Review of DoD Information for Public Release, for more information.

Additional Discussion: If the group has watched the previous two videos, you may ask them to discuss some of the potential risk indicators displayed in those episodes and discuss what an insider threat program is and why it is important.

Indicators from Previous Episodes:

- Splitting up with his girlfriend and calling off their engagement
- Purchasing an expensive car
- Mentioned having financial difficulties
- Unexpectedly submitting his two week notice
- Discouraged because he didn't get the lead programmer position
- Working late, quickly turning off computer screen, and talking quietly to someone on the phone

Additional Discussion: What is an Insider Threat Program?

- Designed to identify "at risk" individuals and help them off this pathway and toward more positive outcomes.
- Insider Threat Programs often assist with solutions that focus on providing help and resources for those in need.
- Insider Threat Programs are multidisciplinary. They typically include representatives from security, counterintelligence, human resources, law enforcement, cyber, behavioral health, and legal. As a team, the group can look at Tim's situation and best determine how to mitigate risk to the organization, including options that would help Tim onto the right path.

Additional Discussion: This is a good point to ask the group if they know how to report information to their Insider Threat Program. The facilitator should provide contact information for their organizational Insider Threat Program.

Additional Facilitator Resources

- Insider Threat Toolkit: https://www.cdse.edu/toolkits/insider/index.php
- Counterintelligence Awareness Toolkit: https://www.cdse.edu/toolkits/ci/index.php
- DoD Insider Threat Trifold: https://www.cdse.edu/documents/cdse/DoD_Insider_Threat_Trifold.pdf
- Insider Threat Case Studies: https://www.cdse.edu/resources/case-studies/insider-threat.html
- Customizable DoD Command Briefing: https://www.cdse.edu/documents/cdse/customizable-dod-command-brief-for-insider-threat-awareness.pdf
- Security Posters: https://www.cdse.edu/resources/posters.html
- Potential Espionage Indicators (PEI): Detecting Actions Outside the Norm Webinar (30 minutes): https://www.cdse.edu/catalog/webinars/counterintelligence/potential-espionage-indicators.html
- Adverse Information Reporting Webinar (30 Minutes): https://www.cdse.edu/catalog/webinars/industrial-security/adverse-information-reporting.html
- Preserving Investigative and Operational Viability in Insider Threat Course (60 minutes): https://www.cdse.edu/catalog/elearning/INT220.html