Insider Threat Mitigation Responses

Student Guide

September 2017

Center for Development of Security Excellence

Lesson 1: Course Introduction

Introduction

Welcome

While Insider Threat Programs may identify individuals committing espionage or other national security crimes, not all incidents will result in the arrest of a spy. In fact, Insider Threat Programs resolve most cases before they escalate into negative events through the proactive identification of individuals at risk of harming the organization—either wittingly or unwittingly—and the deployment of alternative mitigation options. This allows the Insider Threat Program to protect information, facilities, and personnel—and to retain valuable employees.

Welcome to the Insider Threat Mitigation Responses course! This course describes the ability of multidisciplinary insider threat teams to craft tailored and effective responses to specific behaviors or issues.

Multidisciplinary insider threat teams are comprised of subject matter experts from:

- Law enforcement
- Security
- Counterintelligence
- Cybersecurity
- Mental health/behavioral science
- Human resources
- Legal

Case Study

Consider the case of Bryan Minkyu Martin. Martin's excessive gambling and other habits left him in debt. He frequently borrowed money from coworkers and exhibited increasingly stressed behavior. Ultimately he attempted to sell national security information to a foreign government. Luckily, in this instance, the FBI interceded with a sting operation before any information could actually be transmitted. Martin was sentenced to 34 years in prison, reduced in rank, forfeited all pay and allowance, and received a dishonorable discharge from the Navy. After his arrest, he stated that others were aware of his risky behavior and that if only the information had been reported he might have been stopped before attempting to betray his country.

A printable case study is available at the end of this Student Guide.

Objectives

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

- Explain the role of Insider Threat Programs in mitigating the risks posed by insider threats and how Programs mitigate those risks
- Describe factors to consider when formulating a mitigation response to an insider threat incident
- Summarize the ability of multidisciplinary teams to craft mitigation responses tailored to insider threat incidents
- Identify reporting requirements that apply to Insider Threat Programs

Lesson 2: Mitigation Overview

Introduction

Welcome

Had Bryan Martin's actions been reported early, an Insider Threat Program could have employed alternative response options to mitigate the threat. When identified early, Insider Threat Programs can often resolve common workplace issues, such as personal problems, financial issues, and even disgruntlement. This results in positive outcomes for both the individual and the organization.

Objectives

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

- Describe the critical pathway model of insider threat and how it applies to mitigating the threat
- Explain the role of Insider Threat Programs in mitigating the risks posed by insider threats and how Programs mitigate those risks

The Critical Pathway

Potential Risk Indicators

Martin's behavior and activities are examples of potential risk indicators (PRIs). PRIs are observable and reportable behaviors and activities that may be exhibited by those at risk of becoming an insider threat. Specific PRIs come from a variety of sources in the security and intelligence communities and may be specific to your organization.

PRIs share general characteristics with the adjudicative guidelines, which some organizations use to determine insider threat risk. PRIs generally belong to the categories listed here:

- Access attributes
- Professional lifecycle and performance
- Foreign considerations
- Security compliance and incidents
- Technical activity
- Criminal, violent, or abusive conduct
- Financial considerations

- Substance abuse and addictive behaviors
- Judgment, character, and psychological conditions

Behavioral Model of Insider Threat

Dr. Eric Shaw, clinical psychologist and consultant to Federal agencies on insider crime, originated the "critical pathway" model for understanding insider attacks. The components of the model are:

1. Personal Predispositions
2. Stressors
3. Concerning Behaviors
4. Insider Threat-Like Behavior

It begins with personal predispositions and personal and professional stressors, which are often the behaviors that emerge as PRIs. Over time, these factors may combine and increase the risk that an individual may become an insider threat.

Consider the Bryan Martin case. Martin's excessive gambling demonstrated a personal tendency toward risk-taking and fed directly into his financial stressors. Compounding the situation, Martin experienced personal stress, wanting to impress his fiancée's father. These stressors led to concerning behavior by Martin, including frequently borrowing money from friends and colleagues. All of these factors culminated in Martin seeking information beyond his need-to-know and copying and removing classified materials from the workplace in a misguided attempt to alleviate his problems.

The model also demonstrates that there are multiple opportunities to redirect individuals on the pathway into more positive behaviors. For example, if Martin had help with his gambling or his financial issues, his behavior may not have escalated. Early intervention can mean the difference between rehabilitation and negative escalation of behavior.

Role of Insider Threat Programs

Overview

Insider Threat Programs fulfill four functions. First, they deter potential insider threats by instituting appropriate security countermeasures, including awareness programs. Next, they detect individuals at risk of becoming insider threats and then mitigate the risks those individuals pose before the issue escalates. Finally, Insider Threat Programs report information about actual or potential insider threats. Early detection and intervention are the keys to mitigating risks, as demonstrated by the critical pathway model.

Let's examine these in greater detail.

Detection

Detection of PRIs typically occurs through reporting by personnel and monitoring conducted by the Program. Once detected, the PRI becomes the catalyst for Insider Threat Program activities, including information gathering, analysis, reporting, and response.

Intervention

The deployment of mitigation options, or your organization's "response" to the insider threat, depends on multiple variables and the unique nature of the insider threat. The mitigation strategy may include referral outside of the Insider Threat Program when required or actions to mitigate the risk internally.

Note that while some insider threat incidents may warrant referrals and intervention from law enforcement, not all meet reporting thresholds or result in an arrest.

In most cases, proactive mitigation responses provide positive outcomes for the organization and the individual. This allows the organization to protect information, facilities, and personnel and to retain valuable employees, and offers intervention to alleviate the individual's stressors and guide them off the critical pathway.

Effective Mitigation

According to the critical pathway model, without intervention, risky behavior may escalate, causing potential damage to national security, personnel, facilities, or other resources. To be effective, Insider Threat Programs must be attentive to potential issues before they pose a threat, have a risk assessment process in place, address potential issues adequately, and take actions that minimize risk while avoiding those that escalate risk.

Review Activities

Review Activity 1

What does the critical pathway model demonstrate?

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

- ○ Everyone with personal issues is an insider threat and must be monitored closely for the escalation of behavior.
- ○ Personal predispositions and stressors can lead to the escalation of behavior unless the individual's stressors are alleviated.
- ○ An individual displaying potential risk indicators should be permitted to escalate in behavior until arrest and prosecution are viable.

Review Activity 2

How do Insider Threat Programs mitigate risks posed by insider threats?

Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.

- ☐ Detect issues early
- ☐ Follow a risk assessment process
- ☐ Adequately address potential issues
- ☐ Refer all issues to law enforcement

Lesson 3: Response Planning

Introduction

Welcome

Insider Threat Programs must carefully plan their mitigation responses to avoid escalation of risk and to engender a thorough and measured approach to the initiation of punitive action.

Objectives

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

- Identify the primary tenets in responding to insider threat matters
- List possible consequences of inappropriate mitigation responses
- Describe factors to consider when formulating a mitigation response to an insider threat incident

Response Basics

Overview

Insider Threat Programs must follow five primary tenets when planning responses to insider threat incidents, the most important of which is “first, do no harm.” Insider Threat programs must also establish and maintain internal procedures and authorities, avoid alerting the individual that they have been identified as a potential insider threat, protect the individual’s privacy and civil liberties, and preserve chain of custody and properly handle evidence.

Let’s examine these in greater detail.

First, Do No Harm

When an insider threat incident occurs, your Insider Threat Program must carefully assess the situation to avoid exacerbating the situation or increasing risk. Consider whether there is imminent danger to the individual or to others and whether there is an active transmittal of classified information. The Insider Threat Program must thoroughly plan its response before taking action and avoid knee-jerk responses. When planning, communicate and coordinate with your Insider Threat Program team members and other organizational elements.

Establish and Maintain Procedures and Authorities

Your Insider Threat Program must ensure that it has detailed procedures and authorities in place for mitigation response options and should maintain a general response plan that

outlines the overall roles and responsibilities of Insider Threat Program personnel and Hub members or other staff and departments.

Avoid Alerting the Individual

In general, your Insider Threat Program should avoid alerting the individual that they have been identified as a potential insider threat. This allows the Program the time needed to determine an appropriate response, ensures the privacy of the individual, and preserves evidence. Note that in some cases immediate intervention may be required.

Protect Privacy & Civil Liberties

Your Insider Threat Program must consider the individual's privacy and civil liberties when developing mitigation response options. Ensure that personal information is properly handled, accessed, used, reported, and retained in accordance with applicable laws, policies, and regulations.

Preserve Chain of Custody and Evidence

Your Insider Threat Program must ensure that early actions taken in incident response do not interfere with the ability of law enforcement or counterintelligence to conduct investigations or operations, or inhibit future prosecution, in cases that require reporting to external agencies. Work with your general counsel and the referral agency to ensure that any evidence associated with the incident is handled properly and adheres to the proper chain of custody.

The *Preserving Investigative and Operational Viability in Insider Threat* course offers additional information if you would like to learn more. You may register for this course through the Center for Development of Security Excellence (CDSE) website.

Unintended Consequences

Impacts

Your Insider Threat Program's response to insider threat indicators or incidents can have long-reaching effects. Even seemingly viable solutions may have inadequate or negative impacts on the individual, on the morale of other personnel, on the mission of your organization, and on public perception of your organization.

Individuals

Possible negative impacts on individuals include disgruntlement due to an overly aggressive response that makes the individual feel poorly treated, which increases risk, and effects to the career or life of the individual due to poor information handling that persists even if the individual is exonerated of wrongdoing or was falsely accused.

Morale

Possible negative impacts on the morale of other personnel include disgruntlement throughout the organization if others learn of an overly aggressive response. This may result in reduced vigilance and hesitancy to report. Overly weak responses may also deter reporting, as it may make personnel feel that it is pointless to report indicators. In addition, seeing a colleague charged with or convicted of a crime, even when it is necessary, may impact morale.

Mission

A possible negative impact on the mission of the organization includes personnel that circumvent the rules to get their work done due to onerous rule or procedure changes at the organization level.

Public Perception

A possible negative impact on public perception of your organization includes low morale and diminished future recruitment capability due to media coverage on the situation and your response.

Threat Analysis

Overview

Insider Threat Programs must take the time to perform the proper gathering and analysis of data before taking action. If an indicator has a plausible explanation and does not increase the risk associated with an individual, an immediate reaction may do more harm than good. Conversely, even if the risk associated with an individual is elevated, it is not necessarily a precursor to a national security crime or act of violence. An immediate response in these instances may compromise the ability of law enforcement and counterintelligence to pursue inquiries, investigations, or operations.

Let's take a closer look at the considerations to keep in mind during threat analysis.

Analysis Goal

The Insider Threat Program should begin by establishing the goal of analysis. What questions is the team trying to answer? State your purpose clearly and in multiple ways to clarify meaning and scope, and consider breaking the problem down into smaller pieces.

For example, consider these large questions that Insider Threat Programs work to resolve:

- Is the individual currently harming the organization's resources?
- If so, is the harm intentional?
- Is there a risk that the individual will do so in the future?

Breaking these into smaller questions can help you to grasp and manage your goal.

When formulating questions, aim to be clear and precise. Anything is possible, so be specific. A clear and precise question might be to consider whether it is possible that the individual stole classified information.

Focus on questions that are significant, answerable, and relevant, such as, “Did the individual have access to the safe? Does the individual display unexplained affluence?”

Finally, differentiate between questions that have a definitive answer, are a matter of opinion, and require consideration of multiple viewpoints. The question, “Were the individual’s credentials used to log onto the system on a specific date?” has a definitive answer, while the question, “Was the individual upset?” is a matter of opinion. While the answer may be relevant and the Program can aggregate the opinions of multiple people to draw a conclusion, the answer is subjective. Also consider whether other viewpoints might reveal a plausible explanation for an indicator. For example, late night activity on an information system may seem suspicious, but the cybersecurity subject matter expert may identify the activity as a common practice of batch patching and updates scheduled to occur when the system is at its lowest usage.

Fair and Balanced Assessment

Insider Threat Programs must also strive toward a fair and balanced assessment of each case. To do so, first identify and acknowledge your assumptions. Consider whether they are justifiable and how they shape your point of view. Next, seek other points of view and evaluate their merits. Finally, ground all claims with the information available. Ensure that your position is supported by the evidence and is based on relevant information. Critically evaluate your position to determine whether you have considered all of the relevant information, whether your conclusion goes beyond the evidence available, and whether there is an argument to be made against your position.

With these considerations in mind, review the example real-world threat analysis case study below.

Example

The Federal Bureau of Investigation (FBI) knew they had a spy in their midst—but who was it? As the FBI conducted their investigation, they felt sure that the spy could not be one of their own, so they identified Brian Kelley, a CIA agent, as their suspect. They investigated Kelley, including a polygraph and a sting operation, both of which Kelley passed. Rather than conclude that perhaps Kelley was not a spy, the FBI took this as evidence that Kelley was an able, well-trained spy.

Eventually, the FBI acquired intelligence information that identified the true spy as Robert Hanssen, a long-time FBI counterintelligence agent who is now considered the most damaging spy in FBI history. However, until the FBI identified Hanssen, Kelley had

been investigated for years and his career was nearly destroyed. Meanwhile, Hanssen continued to spy and place national security at risk for over 20 years.

How much sooner might the FBI have identified the true threat if the investigators had considered how the assumption that the spy must be CIA influenced their perspective, sought multiple viewpoints, and regarded the evidence available that opposed their viewpoint?

Review Activities

Review Activity 1

How well do you understand the primary tenets of responding to insider threat matters?

For each statement, select whether it is true or false. Then check your answers in the Answer Key at the end of this Student Guide.

It is better to act quickly than to take the time to thoroughly plan a response.

- ○ True
- ○ False

Insider Threat Programs should maintain detailed procedures and authorities.

- ○ True
- ○ False

The Insider Threat Program should notify individuals when they have been identified as a potential insider threat.

- ○ True
- ○ False

Review Activity 2

Leanne's organization terminated her employment after she mistakenly left classified information on the printer. It was her first security violation. Which of the following are possible consequences of this response?

Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.

- ☐ Impacts on Leanne's career
- ☐ Disgruntlement throughout the organization
- ☐ Other personnel less willing to report indicators
- ☐ Impacts on recruitment of new employees

Review Activity 3

Which of the following best describes the considerations for formulating an insider threat mitigation response?

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

- ○ Establish a goal, seek opinions, ask broad questions, consider arguments for and against each position
- ○ Establish a goal, acknowledge assumptions, consider other viewpoints, base conclusions on the evidence
- ○ Act immediately, break the problem into manageable pieces, assume the simplest explanation is most likely to be accurate

Lesson 4: Multidisciplinary Mitigation Responses

Introduction

Objectives

Multidisciplinary insider threat teams are uniquely positioned to craft mitigation responses tailored to specific insider threat incidents.

Multidisciplinary insider threat teams are comprised of subject matter experts from:

- Law enforcement
- Security
- Counterintelligence
- Cybersecurity
- Mental health/behavioral science
- Human resources
- Legal

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

- Differentiate between organizational and individual responses
- Summarize the ability of multidisciplinary teams to craft mitigation responses tailored to insider threat incidents

Types of Responses

Organizational and Individual

Responses to insider threat incidents may be organizational, individual, or both. Organizational responses address a systemic problem with security procedures, training, hiring practices, policies, or other procedures that increase the risk associated with the insider threat. Individual responses address a specific incident and are designed to mitigate the risk associated with or harm caused by a specific individual. In some cases, an organizational response may be effective in addition to or in place of an individual response.

Organizational Response

Examples of organizational responses:

- Changing policy or Standard Operating Procedures (SOP) throughout the organization
- Disabling thumb drives across the organization to prevent downloading sensitive information

- Instituting random bag checks
- Introducing metal detectors
- Providing training or briefings to:
  - Increase awareness of tactics used by adversaries
  - Prevent individuals from becoming unwitting insider threats

Individual Response

Examples of individual responses:

- Internal referrals to human resources or security
- Referral to counterintelligence or law enforcement for inquiry, investigation, or operation
- Referral to counseling, such as mental health or financial
- Punitive actions, such as revocation of access or termination of employment

Tailored Multidisciplinary Mitigation Responses

Overview

The multidisciplinary nature of Insider Threat Programs allows them to craft responses tailored to specific behaviors. A multidisciplinary team working together can provide the most effective responses, which often include a multi-faceted implementation that may include a mix of organizational and individual responses that cover multiple disciplines.

To learn more about the disciplines that comprise a multidisciplinary insider threat team, refer to the *Developing a Multidisciplinary Insider Threat Capability* course. You may register for this course through the Center for the Development of Security Excellence (CDSE) website.

Human Resources (HR)

Example response options specific to human resources:

- Referral to the Employee Assistance Program (EAP) for resources in financial counseling, lending programs, mental health, and other well-being programs
- Medical referrals
- Mediation with supervisors
- Training
- Employee termination procedures
- Other career opportunities

Cybersecurity

Example response options specific to cybersecurity:

- Reduce privileges or system access
- Reconfigure hardware, such as to prevent the use of thumb drives or disc burning
- Limit downloadable file size
- Limit or prevent printing
- Conduct training and awareness campaigns on phishing and other cyber targeting methods
- Increase monitoring

Security

Example response options specific to security:

- Log a security violation or infraction
- Provide security counseling, training, or awareness
- Implement daily bag checks
- Implement random drug and alcohol testing
- Conduct physical monitoring
- Modify Standard Operating Procedures (SOP)

Counterintelligence (CI)

Example response options specific to counterintelligence:

- Referral to the cognizant CI activity for inquiry, investigation, or operation as warranted
- Provide training on foreign targeting methods and recruitment
- Develop a foreign travel brief/debrief program
- Provide threat awareness materials

Law Enforcement (LE)

Example response options specific to law enforcement:

- Referral to the cognizant LE activity for inquiry or investigation as warranted
- Provide criminal threat briefings and awareness materials

Mental Health/Behavioral Science

Example response options specific to mental health and behavioral science:

- Treatment recommendations
- Referral to marital, grief, or other mental health counseling
- Referral to substance abuse rehabilitation programs
- Referral to suicide prevention

Legal

Be sure to include legal in the development of response options to ensure the potential response aligns with privacy protection requirements and other policies.

Response Monitoring

Once the Insider Threat Program implements a mitigation response, it must monitor the response to determine if the risk has been minimized. Note that implementing a mitigation response option does NOT eliminate risk.

Coordinate with your Insider Threat Program partners to determine whether additional mitigation is required. Keep in mind that law or policy may prevent some partners from sharing information with the Program. These may include Employee Assistance Programs, law enforcement, and counterintelligence. As such, the Insider Threat Program should remain vigilant for additional or escalating indicators and document behaviors or activities of concern.

Finally, be sure to periodically re-evaluate the mitigation response to determine if it remains the best option.

Case Study

Recall Bryan Martin, who attempted to sell classified information to alleviate his financial troubles. Let's assume for a moment that a colleague reported Martin's financial problems early on rather than allow his behavior to escalate. What mitigation responses might a multidisciplinary Insider Threat Program have used to proactively redirect Martin away from the critical pathway?

Some possible mitigation responses that may have applied to the Martin case include a combination of:

- Referral to financial counseling to help Martin get his debt under control (individual response; HR)
- Referral to gambling addiction resources to help him get the behavior causing the debt under control (individual response; Mental Health/Behavioral Science)

- Reducing or limiting the ability of personnel within the organization to print or photocopy classified information (organizational response; Cybersecurity)
- Instituting daily bag checks within the organization (organizational response; Security)

Note that mitigation responses are not a one-size-fits-all solution. No two insider threat incidents are alike, even when similar potential risk indicators are present, so be sure your team evaluates each incident on a case-by-case basis.

Review Activities

Review Activity 1

For each mitigation response, select whether it is an organizational or individual response. Then check your answers in the Answer Key at the end of this Student Guide.

Referral to counterintelligence or law enforcement

- ○ Organizational
- ○ Individual

Conduct training and awareness campaigns

- ○ Organizational
- ○ Individual

Issue a security violation

- ○ Organizational
- ○ Individual

Terminate employment

- ○ Organizational
- ○ Individual

Review Activity 2

How do multidisciplinary insider threat teams craft tailored mitigation responses?

Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.

- ☐ Employ response options from multiple disciplines
- ☐ Appoint a discipline to determine the best response depending on the incident
- ☐ Use a mix of individual and organizational responses
- ☐ Maintain a standardized approach to common types of insider threat incidents

Lesson 5: Reporting Requirements

Introduction

Objectives

Insider Threat Programs must report certain types of information. This lesson describes reporting requirements for DoD, Federal, and industry Insider Threat Programs.

Here is the lesson objective. Take a moment to review it.

- Identify reporting requirements that apply to Insider Threat Programs

Reporting

Overview

DoD, Federal agency, and industry Insider Threat Programs operate under different regulations and requirements for reporting. When reporting, your Program may need to cease its activities, such as when the referral agency initiates an inquiry or investigation. In other instances, the Program may be able to employ alternate mitigation options concurrent with external actions. Coordinate with the referral agency and your General Counsel to determine the appropriate steps to take after reporting.

Let's examine the reporting requirements for DoD, Federal, and industry Insider Threat Programs in greater detail.

DoD Requirements

DoD Insider Threat Programs are obligated to report certain types of information to:

- The Federal Bureau of Investigation (FBI)
- The DoD Insider Threat Management and Analysis Center (DITMAC)
- The cognizant Military Department Counterintelligence (MILDEP CI) Office

FBI: Section 811 of the Intelligence Authorization Act requires reporting to the FBI when classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power. To report to the FBI, use the FBI Headquarters email point of contact for secure reporting or contact your local field office.

DITMAC: The DITMAC sets their own reporting thresholds, which are continuously updated based on threats. Contact the DITMAC for the current thresholds. When reporting to the DITMAC, use the DITMAC System of Systems (DSOS).

MILDEP CI Office: Enclosure 4 of DoD Directive (DoDD) 5240.06, Counterintelligence Awareness and Reporting, lists behaviors that DoD entities must report to the MILDEP CI Office, including contacts, activities, indicators, and behaviors related to foreign intelligence, international terrorism, and foreign intelligence entity (FIE) associated cyberspace. Check your organization's procedures for reporting to your cognizant MILDEP CI Office.

In addition, DoD Insider Threat Programs must report adverse information pursuant to the adjudicative guidelines to information systems such as the Defense Information System for Security (DISS) or other databases as required by the organization. DoD Insider Threat Programs must also report criminal activity to the appropriate military or local law enforcement organization. Finally, the Program must comply with any other internal reporting procedures it has established.

Federal Requirements

Federal Insider Threat Programs are obligated to report to the FBI under Section 811 of the Intelligence Authorization Act when classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power.

In addition, Federal Insider Threat Programs must follow any other internal reporting procedures established within the organization.

Industry Requirements

Industry Insider Threat Programs are obligated to report certain types of information to the FBI and the Defense Counterintelligence and Security Agency (DCSA).

The National Industrial Security Program Operating Manual (NISPOM) requires cleared industry to report actual, probable, or possible espionage, sabotage, terrorism, or subversive activities at any location to the FBI and DCSA.

The NISPOM also requires cleared contractors to report adverse information as listed in Chapter 1, Section 302(a) to DCSA.

In addition, industry Insider Threat Programs must report via information systems such as DISS or other databases as directed and follow any other internal reporting procedures as established by their Insider Threat Program.

Review Activity

Review Activity

For each requirement, select whether it applies to DoD, Federal, and industry Insider Threat Programs.

Report to the FBI when classified information is disclosed in an unauthorized manner to a foreign power

- ☐ DoD
- ☐ Federal
- ☐ Industry

Report to the DITMAC

- ☐ DoD
- ☐ Federal
- ☐ Industry

Report adverse information to DCSA

- ☐ DoD
- ☐ Federal
- ☐ Industry

Lesson 6: Course Conclusion

Conclusion

Summary

Insider Threat Programs mitigate the threats posed by witting and unwitting insiders through the deployment of multidisciplinary responses designed to lead the individual away from the critical pathway to becoming an insider threat and reporting information outside of the Program as required.

As you work within your Program to craft tailored and effective mitigation responses, remember that each insider threat incident is unique and should be carefully analyzed and assessed to prevent causing further harm.

Lesson Summary

Congratulations! You have completed the *Insider Threat Mitigation Responses* course.

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

- Explain the role of Insider Threat Programs in mitigating the risks posed by insider threats and how Programs mitigate those risks
- Describe factors to consider when formulating a mitigation response to an insider threat incident
- Summarize the ability of multidisciplinary teams to craft mitigation responses tailored to insider threat incidents
- Identify reporting requirements that apply to Insider Threat Programs

To receive course credit, you must take the *Insider Threat Mitigation Responses* examination. If you accessed the course through the Security Training, Education, and Professionalization Portal (STEPP), please use that system to register for the online exam. Otherwise, select the Take Exam button on the last screen of the course to take the online exam and receive your certificate.

Appendix A: Answer Key

Lesson 2 Review Activities

Review Activity 1

What does the critical pathway model demonstrate?

- ○ Everyone with personal issues is an insider threat and must be monitored closely for the escalation of behavior.
- ⊙ Personal predispositions and stressors can lead to the escalation of behavior unless the individual's stressors are alleviated. *(correct response)*
- ○ An individual displaying potential risk indicators should be permitted to escalate in behavior until arrest and prosecution are viable.

Feedback: *The critical pathway model demonstrates that multiple factors cause insider threat-like behavior and that individuals can be redirected off the path with early intervention.*

Review Activity 2

How do Insider Threat Programs mitigate risks posed by insider threats?

- ☑ Detect issues early *(correct response)*
- ☑ Follow a risk assessment process *(correct response)*
- ☑ Adequately address potential issues *(correct response)*
- ☐ Refer all issues to law enforcement

Feedback: *To effectively mitigate risks, Insider Threat Programs must detect issues early, have a risk assessment process in place, and adequately address potential issues.*

Lesson 3 Review Activities

Review Activity 1

How well do you understand the primary tenets of responding to insider threat matters?

It is better to act quickly than to take the time to thoroughly plan a response.

- ○ True
- ⊙ False *(correct response)*

Feedback: *While some incidents require an immediate response, Insider Threat Programs should thoroughly plan their responses to avoid making the situation worse.*

Insider Threat Programs should maintain detailed procedures and authorities.

- ⊙ True *(correct response)*
- ○ False

Feedback: *Insider Threat Programs should establish and maintain procedures and authorities.*

The Insider Threat Program should notify individuals when they have been identified as a potential insider threat.

- ○ True
- ⊙ False *(correct response)*

Feedback: *Insider Threat Programs should avoid alerting the individual to allow the Program time to develop an appropriate response.*

Review Activity 2

Leanne's organization terminated her employment after she mistakenly left classified information on the printer. It was her first security violation. Which of the following are possible consequences of this response?

- ☑ Impacts on Leanne's career *(correct response)*
- ☑ Disgruntlement throughout the organization *(correct response)*
- ☑ Other personnel less willing to report indicators *(correct response)*
- ☑ Impacts on recruitment of new employees *(correct response)*

Feedback: *All of these are possible consequences of an overly harsh response to this incident.*

Review Activity 3

Which of the following best describes the considerations for formulating an insider threat mitigation response?

- ○ Establish a goal, seek opinions, ask broad questions, consider arguments for and against each position
- ⊙ Establish a goal, acknowledge assumptions, consider other viewpoints, base conclusions on the evidence *(correct response)*
- ○ Act immediately, break the problem into manageable pieces, assume the simplest explanation is most likely to be accurate

Feedback: *When performing analysis for a mitigation response, take the time to plan thoroughly, clarify and be specific with your goals, and strive for a fair and balanced assessment of the case.*

Lesson 4 Review Activities

Review Activity 1

Referral to counterintelligence or law enforcement

- ○ Organizational
- ⊙ Individual *(correct response)*

Feedback: *A referral to counterintelligence addresses a specific incident and aims to mitigate the risk associated with the individual.*

Conduct training and awareness campaigns

- ⊙ Organizational *(correct response)*
- ○ Individual

Feedback: *Training and awareness campaigns address systemic issues across the organization.*

Issue a security violation

- ○ Organizational
- ⊙ Individual *(correct response)*

Feedback: *A logged security violation addresses a specific incident and aims to mitigate the risk associated with the individual.*

Terminate employment

- ○ Organizational
- ⊙ Individual *(correct response)*

Feedback: *Termination of employment is a punitive action that addresses a specific incident and aims to mitigate the risk associated with the individual.*

Review Activity 2

How do multidisciplinary insider threat teams craft tailored mitigation responses?

- ☑ Employ response options from multiple disciplines *(correct response)*
- ☐ Appoint a discipline to determine the best response depending on the incident
- ☑ Use a mix of individual and organizational responses *(correct response)*
- ☐ Maintain a standardized approach to common types of insider threat incidents

Feedback: *Multidisciplinary insider threat teams work together to determine the most appropriate mitigation responses, drawing from their areas of expertise, connections, and various organizational and individual responses.*

Lesson 5 Review Activity

Review Activity

Report to the FBI when classified information is disclosed in an unauthorized manner to a foreign power

- ☑ DoD *(correct response)*
- ☑ Federal *(correct response)*
- ☐ Industry

Feedback: *DoD and Federal Insider Threat Programs must report to the FBI when classified information is or may have been disclosed in an unauthorized manner to a foreign power, per the Intelligence Authorization Act. Industry must report the loss of classified information to DCSA, and espionage, sabotage, or terrorism to both the FBI and DCSA, per the NISPOM.*

Report to the DITMAC

- ☑ DoD *(correct response)*
- ☐ Federal
- ☐ Industry

Feedback: *DoD Insider Threat Programs must report information that meets DITMAC reporting thresholds to the DITMAC.*

Report adverse information to DCSA

- ☐ DoD
- ☐ Federal
- ☑ Industry *(correct response)*

Feedback: *Industry Insider Threat Programs must report adverse information as listed in the NISPOM to DCSA.*

Center for Development of Security Excellence
CDSE
Learn. Perform. Protect.

INSIDER THREAT JOB AID

Awareness in Action: Case Study

Who could become an insider threat? Anyone with authorized access to protected information who uses that access—either wittingly or unwittingly—to harm national security. Insider threats can have far reaching consequences and impacts on national security.

Bryan Martin

Petty Officer 2nd Class Bryan Martin

- Arrested in December 2010 for attempting to sell classified documents to someone he believed was a Chinese intelligence officer
- Pleaded guilty to four counts of attempted espionage
- Age at conviction: 22
  Sentenced to 34 years in prison, reduced in rank, forfeited all pay and allowances and a dishonorable discharge from the Navy.

Insider Threat Indicators

- ***Financial*:** Personal finance problems known to peers
- ***Personal Conduct:*** Excessive gambling and prostitution
- ***Mishandling Classified Documents:*** Removed classified documents and material from secure facilities.

What Happened

- Martin claimed that he was "blinded by greed" when he sold classified documents to a man he believed was a Chinese spy, but was actually an undercover FBI Agent.
- Martin was overextended due to gambling and prostitution debts. He was recently engaged and in an effort to shore up personal finances and impress his father-in-law to be he attempted espionage.
- The undercover agent paid Martin $11,500 in exchange for three packets of documents containing Secret and Top Secret information about current naval operations and intelligence assessments.

Impacts

- The classified information Martin sold to the undercover agent included photos, satellite images and details about U.S. operations in Afghanistan and Iraq.
- Martin revealed his access to military computer systems and named classified network systems he had access to.
- Could have resulted in grave damage to U.S. National Security if the undercover agent was in fact a Chinese foreign intelligence agent.

Learn More

This case study examined a real-life insider threat. Your awareness is key to protecting our national security from insider threats like this one. Visit the Center for Development of Security Excellence's website (http://www.cdse.edu) for additional case studies, information, materials, and training or go directly to the Insider Threat Tool Kit at http://www.cdse.edu/toolkits/insider/index.php

If you SEE something, SAY something.