Behavioral Science and Insider Threat

Course Introduction
Course Introduction

Newscaster: In regional headlines this morning a bomb exploded in a major international shopping district yesterday. Government officials have confirmed that six Americans were among those killed in the attack. The bombing has been linked to the unauthorized disclosure of information involving U.S. activities in the region...

Female 1: Rich…

Rich: Oh, what's going on with Karl?

Female 1: I just heard someone say that someone gave up our classified program but… Karl?

Rich: You don't think it's connected to the bombing, do you?

Female 1: Oh my God, I know he's been stressed lately but if only I could've done something. Could I have prevented this?

Screen text: VIDEO

Sylvia: The preceding video clip was from the National Insider Threat Task Force's Any Given Day video, which can be viewed in its entirety in the Course Resources.

Malicious insiders have caused, and can do, tremendous damage to national security. In many cases, damage could have been avoided if one observant colleague spoke up.

By saving a coworker from making a bad decision, you might be protecting our national security. This course will cover behavioral science and its application to insider threat programs.

Introduction

Narration: Welcome to the Behavioral Science in Insider Threat course! Take a moment to review the course objectives.

Screen text: Behavioral Science and Insider Threat Course

Course Objectives:
- Determine why an organization may require the use of behavioral science to help address potential insider threats
- Explain how behavioral science may be applied to help prevent insider threats in an organization
- Explain how behavioral science is used to determine possible insider threats

Organizational Culture

Insider Threat

Narration: In this lesson, we'll define behavioral science and organizational culture, and relate the importance of organizational culture to behavioral science. Insider Threat is defined in both DoD and National Policy. We'll use the definition from Department of Defense Directive 5205.16.

Insider threat is the threat insiders pose to DoD and U.S. Government installations, facilities, personnel, mission or resources. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

Screen text:

Learning Objectives:
- Define behavioral science
- Define organizational culture
- Relate the importance of organizational culture to behavioral science

DoD Directive 5205.16
Incorporating Change 2

3. POLICY. It is DoD policy that:
   a. DoD will implement the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs in accordance with References (b), (e), (f), and (h).
   b. The threat that an insider may do harm to the security of the United States requires the integration and synchronization of programs across the Department. This threat can include damage to the United States through espionage, terrorism, unauthorized

disclosure of national security information, or through the loss or degradation of resources or capabilities.

Policy and Standards

Narration: Insider Threat Programs are required for federal agencies, DoD components, and cleared industry. These programs are established in accordance with DoD and National Policy. You can access these policies in the Course Resources.

While policies vary slightly based on the nature of your organization, all insider threat program policies require a multi-disciplinary approach to detect, deter, and mitigate insider threat.

This must include law enforcement, counterintelligence, security, human resources, cyber security, and mental health or behavioral science professionals.

Screen text: National Insider Threat Task Force

2009   Fort Hood Shooting
2010
2011   Executive Order 13587
        Wiki Leaks
2012   Presidential Memorandum established the National Insider Threat Policy and Minimum
        Standards for Executive Branch Insider Threat Programs
2013   Washington Navy Yard shooting
2014   DoD Directive 5205.16
2015   DoD Directive 5205.83
2016   NISPOM Change 2
        ISL 2016-02

To learn more about the Executive Order, NITTF Minimum Standards, DoD Insider Threat Program, or the DITMAC, visit the Course Resources.

Knowledge Check

Screen text:

Question 1 of 2
Insider Threat Programs are required to have multi-disciplinary capabilities to include which elements? Select all that apply; then select Submit.

- Cybersecurity
- Counterintelligence
- Behavioral Science or Mental Health
- Human Resources

Insider threat is limited to damage to the United States through espionage or terrorism alone. Select the best response; then select Submit.

- True
- False

Behavioral Science

Narration: As defined in the Merriam-Webster Dictionary, behavioral science is a branch of science (such as psychology, sociology, or anthropology) that primarily deals with human action and often seeks to generalize about human behavior in society.

At its core, it's about human behavior, which cannot be predicted with 100% accuracy. However, by studying human behavior, we can apply a degree of risk management to the process.

Not all organizations have behavioral science personnel; however, they do have the ability to reach out to external resources when needed. Behavioral scientists provide training, consultation, and research, and at times are involved with these aspects simultaneously.

The U.S. Intelligence Community and federal law enforcement are supported by behavioral scientists in numerous ways. Some of these include clinical psychological assessment, personnel security-related consultation, forensic psychology research, and Employee Assistance Program, or EAP, counseling.

In addition to individual behavior, behavioral scientists consider organizational culture and its link to insider threat.

Screen text:

Behavioral science is a branch of science that primarily deals with human action and often seeks to generalize about human behavior in society.

What is behavioral science?
By studying human behavior, we can apply a degree of risk management to the process.

Consultation
Training
Research

- Clinical psychological assessment for incoming and on-board personnel (e.g., psychological fitness for duty
- Organizational psychology focused on such issues as job analysis, selection, performance, leadership development, and climate
- Personnel security-related consultation for insider threat program components (e.g.,

background investigations, counterintelligence)
- For academic and applied research, for example, to identify and validate "indicators" of insider risk
- Forensic psychology research, analysis and consultation in support of criminal investigations
- Specialized operational psychology support (i.e., hostage rescue, counterintelligence, personnel recovery)
- Employee Assistance Program (EAP) counseling and referral services for the general workforce

Organizational Culture

Narration: Organizational culture is the set of underlying beliefs, assumptions, values, and norms of interaction which contribute to the unique social and psychological environment of an organization.

Organizational culture is important because it functions as a "lens" which can influence attitudes, perceptions, behaviors, and expectations in the employee population.

Look at some examples of how organizational culture relates to insider threat prevention, detection and mitigation efforts.

Screen text:

Organizational Culture

Why Is It Important?
- Loyalty, commitment to the mission and the organization
- Conformity with security-related rules and guidelines
- "Organizational citizenship behavior" – voluntary actions geared toward the greater good, independent of personal gain
- Willingness to seek professional help for personal/psychological issues which could decrease reliability or effectiveness
- Vigilance about protecting the organization and national security interests, and reporting concerning or suspicious behaviors if necessary

Knowledge Check

Screen text:

Question 1 of 2
Which of the following terms is identified as a branch of science that primarily deals with human action and often seeks to generalize about human behavior in society? Select the best response; then select Submit.

- Behavioral science
- Insider threat
- Sociology
- Organizational culture

Question 2 of 2
An organization's culture functions as a "lens" which can influence attitudes, perceptions, and behaviors in the employee population. Select the best response; then select Submit.

- True
- False

Lesson Conclusion

Narration: Great job with this lesson and achieving these objectives!

Screen text:

Learning Objectives:
- Define behavioral science
- Define organizational culture
- Relate the importance of organizational culture to behavioral science

Behavioral Scientists

Lesson Objectives

Narration: In this lesson, we'll investigate the role of behavioral science in an insider threat team and how it's applied within insider threat programs. Let's get started.

Screen text:

Learning Objectives:
- Identify the role and value of behavioral science in a multi-disciplinary insider threat team
- Explain how behavioral science is applied within insider threat programs

Insider Threat Program

Narration: How can Behavioral Scientists contribute to Insider Threat Programs?

Psychologists and other behavioral scientists add value by helping identify, explain, and

contextualize concerning behaviors that come to the attention of an Insider Threat Hub. They can provide expert consultation, training, and customized analytical tools to help distinguish between mere troubled employees and those presenting a genuine threat.

Finally, behavioral scientists can operationalize current research to enhance an organization's insider threat deterrence, detection, and mitigation efforts. Behavioral science utilizes many different methods and types of information, including empirical, observational and clinical data.

In its Insider Threat Program Maturity Framework, NITTF addresses the importance of behavioral science in two of its 15 maturity framework elements, or MEs. In ME5, the NITTF Maturity Framework states that continuing education and training for Insider Threat Program personnel is vital to maintain currency and methodologies in the program disciplines. Among the most important are behavioral sciences and analytic methodologies, data analytics, security, privacy and civil liberties, and counterintelligence.

ME15 adds that the human-centric nature of the insider threat issue increases the importance of incorporating behavioral science perspective and expertise into an Insider Threat Program.

A program with access to behavioral sciences expertise, either through internal departments and agencies or affiliated resources, can strengthen its capabilities to identify and assess types of concerning behavior, discern subconscious biases, and propose alternative hypotheses.

Personnel with this expertise may provide additional context and insight into social/cultural mores that may impact mitigation strategies and furnish advice during periodic revisions to insider threat indicators, triggers, and thresholds.

Screen text: How Can Behavioral Scientists Contribute to Insider Threat Programs?

Identify
Explain
Contextualize

Research
- Empirical
- Observational
- Clinical data

ME5
Includes stakeholders from a broad range of functional areas and others with specialized disciplinary expertise to strengthen Insider Threat Program processes.

- Continuing education and training for Insider Threat Program personnel is vital to maintain currency and methodologies in the program disciplines
- Behavioral sciences and analytic methodologies, data analytics, security, privacy and civil liberties, and counterintelligence

ME5
Employs behavioral science methodologies to help identify indicators of potential insider threats.
- Includes stakeholders from a broad range of functional areas and others with specialized disciplinary expertise to strengthen Insider Threat Program processes.

Strengthen its capabilities to:
- Identify and assess types of concerning behavior
- Discern subconscious biases
- Propose alternative hypothesis

To learn more about the NITTF Maturity Framework, visit the Course Resources.

Insider Threat Program (cont.)

Narration: Research is a critical aspect of behavioral science. Researchers conduct interviews, review case studies, and analyze data. One such organization that conducts research and development is the Defense Personnel and Security Research Center, or PERSEREC.

PERSEREC, in its recently released technical report or TR 18-16, titled, "A Strategic Plan to Leverage the Social and Behavioral Sciences to Counter the Insider Threat" cites this: "Insider Threat Programs recognize 'the humanity of human behavior' — the messiness, the inconsistency, and the adaptability — and in collaboration with other stakeholders, develop structured and supported interventions for those that may pose a potential threat. Social and behavioral scientists are well-positioned to contribute to this mission by delivering robust empirical research and actionable, relevant recommendations to guide policy and practice."

Screen text:

PERSEREC

Conclusion
In the words of one government SME, successful ITPs recognize "the humanity of human behavior" – the messiness, the inconsistency, and the adaptability – and in collaboration with other stakeholders, develop structured and supported interventions for those who may pose a potential threat. Social and behavioral scientists are well-positioned to contribute to this mission space by delivering robust empirical research and actionable, relevant recommendations to guide both policy and practice.

Dr. Gallagher

Narration: Let's listen to a conversation with Dr. Robert Gallagher of the DoD Insider Threat Management and Analysis Center about behavioral science and the role behavioral scientists play in an insider threat program.

VIDEO

[Rebecca Morgan:] So many people have had the requirement to stand up an insider threat program and that has applied to DoD components, to federal agencies as well as to our industry partners under the NISPOM. And, all of them had a requirement to include a mental health professional or SME as part of the hub or the program management team.

But I'm not sure everybody knows exactly what that means or what they would do. So you are providing a role as a behavioral scientist at the DITMAC, do I have that right? [Dr. Gallagher:] Correct.

[Rebecca Morgan:] Awesome, okay and so can you expand a little bit for us what the role of behavioral science is in an insider threat program?

[Dr. Gallagher:] Sure so, the logic behind involving behavioral science is that insider threat is essentially a human behavior issue; people make a choice to act in a certain way. And so, the more we understand about why people do what they do, the better we can mitigate and control that kind of behavior. So, when you involve a behavioral scientist there are a number of ways that behavioral scientists can contribute.

The first one is in a consultative role. So consulting to analysts, leadership or anyone else in the insider threat domain and helping them understand the context and the culture in which the behavior is occurring, the things that might drive that behavior. And, then the more we know about that, the more we can do about it.

[Rebecca Morgan:] And just to add, so when you say consultative role you are not talking about consulting with the client as if you were a therapist, you're talking about working with the other members of the insider threat program.

[Dr. Gallagher:] Yes, of being part of that decision-making body of the team that's looking at the behavior, trying to understand the context and the terms of the behavior. And that would be the role of the behavioral scientists in that part of the picture. There's also roles for behavioral scientists in research, trying to understand the larger context of why people do what they do and especially as it relates to insider threat and there is a lot of vibrant research going on today.

Psychologists or other types of behavioral scientists are frequently involved at EAPs or other types of care facilities and so they will be involved in evaluating the individuals when they present with a potential mental health challenge or a question about their stability. They'll be involved in evaluating and treating that individual. And then the last place where psychologists or other types of behavioral scientists can get involved is typically in training.

So, within the DITMAC I do a regular training series and we've done things, topics ranging from the process of radicalization to the indicators of violence and suicide. So, things along those lines are the primary ways that a behavioral scientist would function.

Narration: In this webinar, Dr. Gallagher explained the roles of behavioral science in an Insider

Threat Program. Behavioral scientists can provide consultation to the program, make recommendations for individual treatment plans, support training and awareness, and conduct research.

Let's explore some of the primary approaches behavioral scientists use in research.

Screen text:

- Provide consultation to the program
- Make recommendations for treatment plans
- Support training and awareness
- Conduct research

Lists

Narration: Everyone makes lists and finds them useful, right?

Individuals may think that a list of indicators is enough for discerning between an insider threat and a non-malicious actor. A cursory search turned up more than 20 distinct lists of behavioral indicators which vary in size from a handful to hundreds of items.

There are three primary approaches to list development: reverse engineering cases, the rational approach, and science.

Reverse engineering cases involves identifying and studying precursors to action in known insider threat cases. However, this approach can lead to backward orientation.

The rational approach is where a subject matter expert, or SME, will rely on logic and experience.

Science is those items that discriminate between good and bad actors. The study of human behavior is complex, and humans are, in a sense, "messy".

An indicator in one setting may not be an indicator in another. An indicator for one person may not be an indicator for another. An indicator for me one day may not be an indicator on another day.

Science can lead to false positives. The base rate of insider threat is very small. For almost any indicator there will be more non-malicious actors than malicious ones.

Just think, if we had a single, comprehensive list of ALL behavioral indicators of insider threat, we could screen for or monitor those indicators and eliminate all insider threats. But it isn't that

simple. Lists tend to treat all indicators as equally indicative and minimize critical thinking. Individuals tend to focus on and minimize selected items.

Screen text:

An indicator is an observable or reportable behavior or activity. Potential risk indicators of insider threat fall under numerous categories. For more information, view the job aids in Course Resources.

1. Reverse Engineering Cases – Involves identifying and studying precursors to action in known insider threat cases.
2. The Rational Approach – A subject matter expert, or SME, will rely on logic and experience.
3. Science – Those items that discriminate between good and bad actors.

- An indicator in one setting may not be an indicator in another.
- An indicator for one person may not be an indicator for another.
- An indicator for me one day may not be an indicator on another day.

- Treat all indicators as equal
- Minimize critical thinking
- Focus on selected items

Knowledge Check

Screen text:

Question 1 of 2
Which of the following do behavioral scientists contribute to Insider Threat programs? Select all that apply; then select Submit.

- o Identifying concerning behaviors
- o Providing expert consultation
- o Monitoring login attempts
- o Employee Aid Program counseling

Question 2 of 2
Which of the following are vital aspects of research in behavioral science? Select all that apply; then select Submit.

- o On-boarding new hires
- o Conducting interviews
- o Analyzing data

  o Reviewing case studies

Lesson Conclusion

Narration: Keep up the good work. Let's move on to the next lesson!

Screen text:

Learning Objectives:
- Identify the role and value of behavioral science in a multi-disciplinary insider threat team
- Explain how behavioral science is applied within insider threat programs

Critical Pathway

Introduction

Narration: Now, you'll learn about the critical pathway and how it relates to insider threats. Review the lesson learning objective.

Screen text:

Learning Objective:
- Explain the critical pathway as it relates to insider threats

FBI Video Trailer

Narration:
[Narrator 1:] Would you characterize your relationship with colleagues as friendly? [Narrator 2:] Would you describe them as troubled? [Male 1:] Hey, this is Doug we're talking about. [Female 1:] He's changed.

[Female 2:] You never do anything! [Male 2:] It's the same old story from you, I'm getting sick of it.

[Female 3:] Did you ever meet this woman? [Male 3:] Did you see anything that would make you suspicious that he was compromising this country to our enemies? [Male 4:] The complaint alleges that Collins conspired to and did commit espionage for a foreign power.

[Male 1:] They will have a bomb by the end of the year and we are not prepared to meet that threat. [Narrator 3:] Once you release classified information you have no control where it ends up.

[Male 5:] The technology cuts both ways. [Male 1:] It was you, wasn't it? [Male 5:] Antidote or weaponry. [Male 1:] In law enforcement, you trust your partner. [Female 1:] Well in intelligence, you err on the side of your country.

Male 1:] These people are helping to keep America safe. Doug's a true patriot. [FBI:] FBI, let me see your hands! [Male 1:] Are you sure? [Female 1:] I have something that I need to talk to you about.

Screen text: BETRAYED

Application of the Critical-Path

Narration: Critical-path analysis has been an approach used in business and medical fields to identify the interrelationship of processes and their most critical and vulnerable points.

Eric Shaw and Laura Sellers drew on recent and comprehensive empirical studies of hostile insider acts — from formal academic efforts to a collection of in-depth case reports — to demonstrate a common set of factors and similar pattern of individual and organizational behavior.

They described these factors and indicators of heightened risk and placed them in the context of a critical-path analysis.

Although behavioral scientists supporting the U.S. Government insider threat mission have varied skill sets and professional backgrounds, their efforts are strengthened by a unifying framework for understanding insider risk.

The critical-path framework provides useful categories for assessing if a given person of concern could be on a destructive path. Fortunately, while most employees experiencing high stress do not betray their country, associated symptoms (like poor concentration) can increase the risk of unintentional threat.

In addition, there are some individuals whose negative predispositions (for example: impulsivity/recklessness) in combination with certain personal, financial, and/or job-related pressures increase the risk of destructive insider activity.

Let's discuss these and the four elements of the critical pathway.

Screen text:

Personal Predispositions
      medical/psychiatric conditions
      undiagnosed and untreated medical conditions
      social network risks
      previous rule violations

personality or social skills issues
decision-making deficits

Stressors
personal
financial
professional

Concerning Behaviors
interpersonal
technical
financial
personnel
mental health
social networks
suspicious travel

Hostile or Destructive Acts

Personal Predispositions

Narration: The first of the four elements is personal predispositions.

Most people do not commit hostile insider acts. There are certain personal characteristics that predispose individuals toward becoming an insider risk. These characteristics include medical/psychiatric conditions, undiagnosed and untreated medical conditions, social network risks, previous rule violations, personality or social skills risks, and decision-making deficits.

However, not everyone with these issues is an insider threat.

Screen text:

Personal Predispositions
medical/psychiatric conditions
undiagnosed and untreated medical conditions
social network risks
previous rule violations
personality or social skills issues
decision-making deficits
Normal and well-adjusted people do not commit hostile insider acts

Not everyone with these issues is an insider threat

Stressors

Narration: Stressors in people's lives can result in changes in personal, social, or professional responsibilities that require effort and energy to adjust.

While everyone experiences stress, research indicates that stressors place additional pressure on those who possess certain vulnerable predispositions and can lead such individuals down the next step on the critical-path.

Again, not everyone with these issues is an insider threat.

Screen text:

Stressors
        personal
        financial
        professional

Stressed?

Not everyone with these issues is an insider threat

Concerning Behaviors

Narration: Studies of inside offenders have shown that most were known to have exhibited some form of concerning or problematic behavior before acting directly against their organization.

These concerning behaviors can be interpersonal, financial, or mental health related to name a few.

Screen text:

Concerning Behaviors
        interpersonal
        technical
        financial
        personnel
        mental health
        social networks
        suspicious travel

Problematic Organizational Responses

Narration: The last element in the critical-path model is problematic organizational behavior in response to at-risk employees, including inaction, inattentiveness, and lack of understanding of the previously addressed factors.

These include inattention, no risk assessment process, and summary dismissal or other actions that escalate risk.

Screen text:

Concerning Behaviors
    interpersonal
    technical
    financial
    personnel
    mental health
    social networks
    suspicious travel

Problematic Organizational Response
    Inattention
    No risk assessment process
    Inadequate investigation
    Other actions escalate risk

Actions that escalate risk

Hostile or Destructive Acts

Narration: While some individuals may act impulsively, the commission of a crime or hostile act usually occurs with planning and preparation. Planning and preparation might involve surveillance or research; solicitation of the cooperation of witting or unwitting others; the acquisition of resources or skills; rehearsal of activities to gauge a plan's safety and effectiveness; attempts at authorized or unauthorized access to obtain, replicate, and transfer targeted information; and deception or other forms of operational security.

Take a look at the case of Aaron Alexis and how the critical-path aligned with his situation.

Screen text:

Concerning Behaviors
    interpersonal
    technical
    financial

personnel
mental health
social networks
suspicious travel

Problematic Organizational Response
Inattention
No risk assessment process
Inadequate investigation
Other actions escalate risk

Hostile or Destructive Acts

- Surveillance or research
- Solicitation of the cooperation of witting or unwitting others
- The acquisition of resources or skills; rehearsal of activities to gauge a plan's safety and effectiveness
- Attempts at authorization or unauthorized access to obtain, replicate, and transfer targeted information
- Deception or other forms of operational security

The "Critical-Path" to Insider Threat Risk source: Shaw, E and Sellers, L (2015)

Not Everyone With These Issues is an Insider Threat

The organizational response and hostile actions:
Aaron Alexis's violence risk and psychiatric problems were documented in police records that neither a security clearance organization or his employer access – he had never been convicted of a crime.

Had they possessed this information prior to employment counselling, the risk to Washington Navy Yard would probably have been avoided.

To learn more about the Critical Pathway, visit the Course Resources

Knowledge Check

Screen text:

Question 1 of 2
Which of the following critical-path elements is described as personal characteristics that predispose individuals toward becoming an insider risk? Select the best response; then select Submit.

- Personal predisposition
- Stressors
- Concerning behaviors
- Problematic organizational responses

Question 2 of 2
Which of the following critical-path elements is best described as an event that results in changes in personal, social, or professional responsibilities that require people to spend effort and energy to adjust? Select the best response; then select Submit.

- Hostile acts
- Concerning behaviors
- Stressors
- Personal predisposition

Lesson Conclusion

Narration: Success! You've completed this lesson.

Screen text:

Learning Objective:
- Explain the critical pathway as it relates to insider threats

Course Conclusion

Conclusion

Narration: The insider threat problem is neither new nor easy to address. Before Private Manning and Reality Winner, there was Ana Montes. Before Major Hasan and Aaron Alexis, there was Sergeant Kreutzer.

Whether it manifests as espionage, unauthorized disclosure, workplace violence, or some other malicious behavior, the insider threat is, at its core, a human problem that results from a complex interplay among individual, interpersonal, and organizational factors.

The Insider Threat Program should be a shared responsibility rather than an exclusive preserve of highly-specialized experts. We must share and collaborate resources. Everyone can play a role in not only preventing insider threat but helping those who may become one.

Screen text:

Insider Threats

Ana Montes
DIA Senior Analyst
2001 – Committed espionage for Cuba

Sergeant Kruetzer
U.S. Army
1995 – Fort Bragg, North Carolina shootings

Major Hasan
U.S. Army
2009 – Fort Hood, Texas shootings

Private Manning
U.S. Army
2010 – WikiLeaks

Reality Winner
Defense Contractor
2017 – Unauthorized Disclosure

- Espionage
- Unauthorized disclosure
- Workplace violence

Insider Threats
Individual, interpersonal, and organizational factors

Video

Narration: [Newscaster:] Moving now to international news. In the Middle East, U.S. officials are attributing a decline in violence to the enhanced communication and cooperation between coalition forces and rebel factions that are holding key cities.

[Female 1:] Karl seems more himself lately… [Rich:] Yeah.

[Newscaster:] And good news for the regional economy. A trade agreement has been approved; all parties are expressing optimism that the new effort will increase safety and stability in the region. We'll return after these messages.

Screen text: 8:23 a.m. – Present Day

Narrator: Malicious insiders have done, and can do, tremendous damage to national security. In many cases, damage could have been avoided if one concerned, observant colleague spoke up.

Leveraging behavioral science professionals as part of a multi-disciplinary insider threat program may help save a coworker from making a bad decision and protect our national security.

To learn more about this topic, we invite you to register and view the following CDSE webinars.

Screen text: Malicious insiders have done, and can do, tremendous damage to national security. In many cases, damage could have been avoided if one concerned, observant colleague spoke up.

Leveraging behavioral science professionals as part of a multi-disciplinary insider threat program may help save a coworker from making a bad decision and protect our national security.

To learn more about this topic, we invite you to register and view the following CDSE webinars.

Behavioral Analysis-Insider Threat Program Webinar
Guest Speaker Dr. Robert Gallagher of the Defense Insider Threat Management and Analysis Center, or DITMAC, discusses this topic and provided his insight on what this discipline brings to insider threat detection and mitigation.

Applied Research on Mental Health Conditions and Security Webinar
Guest Speakers Dr. Eric Lang and Rene Dickerhoof of the Department of Defense Personnel Security Research Center host a discussion regarding research of assessing and managing mental health issues related to personnel security, suitability, and insider threat.

Course Conclusion

Narration: Awesome job with this course!

Screen text: Congratulations!
Behavioral Science and Insider Threat

Answer Key

Lesson 1
Insider Threat Programs are required to have multi-disciplinary capabilities to include which elements? Select all that apply; then select Submit.

- Cybersecurity
- Counterintelligence
- Behavioral Science or Mental Health
- Human Resources

Insider threat is limited to damage to the United States through espionage or terrorism alone. Select the best response; then select Submit.

- False

Which of the following terms is identified as a branch of science that primarily deals with human action and often seeks to generalize about human behavior in society? Select the best response; then select Submit.

- Behavioral science

An organization's culture functions as a "lens" which can influence attitudes, perceptions, and behaviors in the employee population. Select the best response; then select Submit.

- True

Lesson 2
Which of the following do behavioral scientists contribute to Insider Threat programs? Select all that apply; then select Submit.

- Identifying concerning behaviors
- Providing expert consultation

Which of the following are vital aspects of research in behavioral science? Select all that apply; then select Submit.

- Conducting interviews
- Analyzing data
- Reviewing case studies

Lesson 3

Which of the following critical-path elements is described as personal characteristics that predispose individuals toward becoming an insider risk? Select the best response; then select Submit.

- Personal predisposition

Which of the following critical-path elements is best described as an event that results in changes in personal, social, or professional responsibilities that require people to spend effort and energy to adjust? Select the best response; then select Submit.

- Stressors