Behavioral Science and Insider Threat Short

Student Guide

June 2026

Center for Development of Security Excellence

Contents

Welcome

Narrator: Welcome, and thank you for joining the Behavioral Science and Insider Threat Q&A session. Insider Threat Hub teams are made up of professionals from:

- Behavioral Science
- Security
- Human Resources
- Legal
- Counterintelligence
- Cybersecurity
- Law Enforcement

Each of these multidisciplinary groups contributes important and unique information to the risk management process.

Insider Threat Hub teams exist to deter personnel from becoming an insider threat, detect existing insider threats, and analyze potential threats to validate reports and develop context on the subject and situation. Insider Threat Hub teams mitigate the risks personnel may pose and work to move them off the critical pathway through early intervention, proactive reporting, and referrals.

Behavioral analysts recognize the human element behind insider threats. They work to assess potential threats by analyzing the reasons behind insider threat behaviors. The insights they provide help mitigate potential threats and determine root causes to help prevent future incidents. For these reasons and more, behavioral scientists are valuable to Insider Threat Hub teams.

Today, you will hear from a Behavioral Science professional and have an opportunity to ask questions to summarize the role Behavioral Science personnel play in deterring, detecting, analyzing, and mitigating potential insider threats.

Behavioral Science Representative Introduction

Narrator: I'd like to introduce our Behavioral Science representative, Dr. Phillip Atkinson. As a Senior Behavioral Science Advisor for the Defense Counterintelligence and Security Agency, or DCSA, Dr. Atkinson applies behavioral science to assess and manage threats for national security operations in the intelligence community and for special operations missions. He has experience as a clinical psychologist for the U.S. Army and as an operational psychologist supporting risk assessment efforts for special operations and counterintelligence missions.

General Behavioral Science and Insider Threat

Narrator: Let's first focus on establishing the basic relationship between Behavioral Science and insider threat.

What is the primary role of a behavioral scientist in an insider threat hub?

Dr. Atkinson: Yeah, so a behavioral scientist in an insider threat hub is a social science expert, typically with a master's degree or doctorate in psychology or sociology or anthropology, and they help the organization understand the human element behind insider threats. Now, while their roles can differ depending on their expertise and the organization they work in, behavioral scientists from various backgrounds can conduct behavioral research, consult on organizational dynamics, and analyze behavioral trends related to insider threats.

Now, when analyzing the behaviors of a specific person of concern, insider threat hubs utilize licensed mental health practitioners with expertise in behavioral threat assessment and management. Licensed professionals, such as psychologists or psychiatrists or social workers, can assess an individual's actions and provide context to help distinguish between behaviors that are simply unusual, versus those behaviors that elevate concern for malicious insider acts. These practitioners who specialize in threat assessment can use their expertise to help the team understand the "why" behind an individual's actions and to assess the potential risk they may pose.

Behavioral scientists contribute to all aspects of insider threat programs, from prevention and detection to mitigation and management. In the prevention phase, behavioral scientists might help develop training and awareness materials or conduct organizational research to determine areas of behavioral risk. For detection, psychologists can help identify and interpret concerning behaviors. In the mitigation phase, their insights are crucial for crafting organizational responses that address the root cause of behavior and de-escalate the situation rather than making it worse.

What is the difference between a behavioral scientist and a data analyst in an insider threat hub?

Dr. Atkinson: While both roles involve analysis, a behavioral scientist focuses on the "why" behind the data, while the data analyst focuses on the "what". A data analyst is skilled in using tools to collect, process, and find patterns in large data sets, such as network logs and user activity. They are experts in identifying anomalies and deviations from normal patterns. A behavioral scientist, on the other hand, takes the data and applies their understanding of human psychology and behavior to interpret its meaning. They provide the context that helps the team understand whether an

anomaly is a genuine threat or simply an unusual, but probably harmless, action. For example, a data analyst might flag that an employee is downloading a large volume of files, but a behavioral scientist could help determine if this is a sign of malicious data exfiltration or a legitimate action due to a new project.

How does behavioral science reframe the insider threat problem?

Dr. Atkinson: Behavioral science reframes the insider threat problem by shifting the focus from a purely technical issue to a human-centric one. Instead of viewing insiders as just another type of security vulnerability, it treats them as individuals whose behavior is influenced by a complex interplay of psychological, and social, and situational, and organizational factors. This approach recognizes that destructive acts are often the end result of a process, not a spontaneous event, and that understanding this process is key to effective prevention and mitigation. Now, by applying principles from psychology, sociology, anthropology, and other related fields, behavioral science helps an insider threat hub move from simply monitoring for suspicious network activity. It encourages looking at the “why” behind an employee's actions, considering factors like stress, disgruntlement, or unmet expectations. And this reframing is crucial because it opens opportunities for early intervention, allowing an organization to offer support to a struggling employee before their behavior escalates into a security incident, turning a potential threat into a success story for both the individual and the organization.

What behavioral science models are used to understand and identify potential insider threats?

Dr. Atkinson: So, beyond the critical pathway, another foundational model used in insider threat is the Pathway to Intended Violence, which was specifically developed to understand an individual's progression towards acts of targeted violence. This model’s been well validated in the scientific research literature and shows how a person of concern can begin with a grievance and then escalate to violent ideation, research and planning, preparation, and to ultimately commit an act of violence and an attack. The Pathway to Intended Violence helps threat assessors determine the level of concern for potential violence so they can most effectively intervene to mitigate the threat.

Behavioral scientists may also conceptualize cases using the Fraud Triangle, which identifies three elements that are often present in cases of occupational fraud: pressure, opportunity, and rationalization. Pressure refers to the motivation or incentive for the act, such as financial hardship. Opportunity is the ability to carry out the act, often due to weak internal controls. And then rationalization is the justification the individual uses to make the act seem acceptable to themselves.

More recent frameworks, like the Sociotechnical and Organizational Factors for Insider Threat, or SOFIT, ontology, provide a comprehensive knowledge base of both technical and behavioral indicators. This model helps to structure the analysis of a wide range of data points, from an employee's psychological state to their interactions with the organization's technical systems.

Additionally, some approaches now incorporate what's called the “dark triad” of personality traits, which includes narcissism, Machiavellianism, and psychopathy. So, they use this as potential risk indicators, as these traits are correlated with a higher likelihood of rule breaking and unethical behavior.

How does behavioral science help mitigate bias and ensure fairness in insider threat programs?

Dr. Atkinson: Behavioral science plays a critical role in making insider threat programs more objective and fair by actively identifying and mitigating cognitive biases. Everyone is susceptible to biases, such as confirmation bias, which could lead them to focus only on information that supports a preliminary judgment. Behavioral scientists train analysts to recognize these biases and use structured analytic techniques and alternative hypothesis to ensure a more balanced and evidence-based assessment. Moreover, the application of behavioral science emphasizes that indicators are not proof of malicious intent and that context is key. It pushes the program to avoid creating a checklist mentality where an employee is flagged simply for exhibiting a certain number of indicators. By mandating a multidisciplinary review that includes behavioral expertise, the program ensures that decisions are not made in a vacuum and that the privacy and civil liberties of employees are protected throughout the process.

Behavioral Science’s Methods of Support for Insider Threat Hubs

Narrator: Let’s move on to a new topic: Behavioral Science’s Methods of Support for Insider Threat Hubs.

What is the “Critical Pathway to Insider Risk” and how do behavioral analysts use it?

Dr. Atkinson: So the critical pathway to insider risk is a conceptual model that describes the stages an individual might go through before committing a malicious act. It starts with personal predispositions, which are underlying traits or vulnerabilities, such as financial problems or a history of rule violations. These are then exacerbated by stressors, which can be personal or professional. And this can lead to concerning behaviors, which are observable actions that deviate from the

norm. And the final step is the problematic organizational response, which is how the organization handles the concerning behavior they observe.

A behavioral scientist can use this model to understand where an individual might be on this path and to identify opportunities for intervention. By recognizing the signs at each stage, they can help the Insider Threat Hub to provide support and resources to the individual before their behavior escalates. The goal is to guide the person off the critical pathway and toward a more positive outcome, both for the individual and the organization.

How does behavioral science inform preventative *measures and help create a culture of trust?*

Dr. Atkinson: So behavioral science is fundamental to creating a proactive, preventative insider threat program. Its principles are used to design training that goes beyond simple rule memorization and instead educates the workforce to recognize concerning behaviors in their peers. And this leverages the trusted workforce as the first line of defense, based on the understanding that colleagues are often the first to notice when someone's struggling.

Furthermore, a behavioral scientist uses these principles to foster a positive organizational cultures where employees feel valued and psychologically safe. By advocating for bidirectional loyalty, organizational justice, and promoting resources like Employee Assistance Programs (or they're called EAPs), the behavioral scientist helps reduce the stressors and feelings of disgruntlement that often lead to insider threats. And this proactive, supportive approach builds trust, encourages employees to report concerns without fear of retaliation, and makes them partners in securing the organization.

How does behavioral science improve the detection *of insider threats?*

Dr. Atkinson: Behavioral science enhances detection by adding crucial context to technical data. Instead of just looking for technical indicators, this approach seeks to understand the motivations, stressors, and psychological factors (so the “why” behind an individual's actions). It moves beyond a purely technical view by integrating observable behavioral indicators, such as personality changes or expressions of disgruntlement, with technical alerts. While a monitoring tool can flag an anomaly (the “what”), behavioral science provides the framework to interpret the data in light of the employees, stressors, performance reviews, or other life events (so the “why”). This whole-person approach helps distinguish between a troubled employee versus someone who's a genuine threat, which reduces false positives and allows the hub to focus its resources on the most credible concerns.

What is User and Entity Behavior Analytics (UEBA) and how do behavior analysts use it?

Dr. Atkinson: User and Entity Behavior Analytics is a type of security technology that uses machine learning and data analytics to model the normal behavior of users and devices on a network. It then flags any activity that deviates from this established baseline. For example, a user analytics tool could alert the security team if a user logs in from an unusual location or accesses files they've never touched before. A behavior analyst uses the output of user analytics tools as a starting point for their analysis. The alerts from a user analytic system provide the "what" and the behavior analyst then investigates the "why". They use their expertise to contextualize the anomaly, looking at the individual's history, job role, and recent stressors to determine if the behavior is truly a cause for concern.

What is the role of behavioral science in the* response and mitigation *phase?

Dr. Atkinson: In the response and mitigation phase, behavioral science is crucial for developing tailored and effective interventions. The goal is to de-escalate the situation and address the root causes of the concerning behavior rather than implementing a one-size-fits-all punitive response that could actually make things worse. A behavioral scientist can help determine the most appropriate course of action, which could range from a referral to an EAP for personal issues, to mediation for a workplace conflict. And this approach is grounded in the critical pathway model, which shows that a problematic organizational response can be the final factor that pushes an at-risk individual toward a malicious act. By using behavioral science insights, the Insider Threat Hub can craft responses that are seen as supportive and fair, guiding the employee away from the destructive path. This not only mitigates the immediate threat, but also reinforces a positive organizational culture where employees feel safe to seek help.

Key Skills for Behavioral Science Insider Threat Hub Team Members

Narrator: I know you have additional questions about the skills required of Behavioral Science members of the Insider Threat Hub Team.

What are some of the key skills a behavioral scientist needs to be effective in an insider threat hub?

Dr. Atkinson: So, an effective behavioral scientist in an insider threat hub needs a unique blend of technical and soft skills. They need to have a strong understanding of behavioral science principles, including psychology and sociology, but they should also have strong analytical skills and the ability to interpret complex data from various sources. And in addition to these technical skills, a behavioral scientist must

have excellent communication and interpersonal skills. They need to be able to communicate their findings clearly and concisely to a variety of audiences, from technical analysts to senior leadership. They also need to be able to build trust and rapport with stakeholders across the organization, as they'll often need to work with HR or Legal and other departments to gather information.

How does a behavioral scientist collaborate with other members of an insider threat hub?

Dr. Atkinson: A behavioral scientist is a key member of a multidisciplinary insider threat team and collaborates closely with experts from other fields, including Cybersecurity, Law Enforcement, and Human Resources. They work with data analysts to interpret the output of technical monitoring tools, providing the behavioral context needed to understand the significance of any anomalies. They also collaborate with investigators to help guide inquiries, ensuring that they're conducted in a way that is sensitive to the individual's privacy and civil liberties. When it comes to mitigation, the behavior analyst works with HR and Legal to develop responses that are appropriate to the situation and that address the root causes of the behavior. This collaborative approach ensures that the Insider Threat Program takes a holistic view of the problem and develop solutions that are both effective and fair.

What are the ethical considerations for a behavioral scientist working in an insider threat hub?

Dr. Atkinson: A behavioral scientist in an insider threat hub must navigate a number of complex ethical considerations. One of the most important is the need to balance the organization's security with the individual's right to privacy. Monitoring employee behavior can be intrusive, and it's essential that it is done in a way that's transparent and respectful of individual privacy. Behavioral scientists have a key role to play in ensuring that the program's activities are conducted in an ethical and responsible manner. Another ethical consideration is the potential for bias in the analysis of behavior. A behavioral scientist must be aware of their own biases and take steps to mitigate them. They should also be sensitive to cultural and individual differences that may influence behavior, and the goal is to make a fair and objective assessment of the individual's risk based on the evidence and to avoid making assumptions or jumping to conclusions.

Conclusion

Narrator: I'd like to wrap up this Behavioral Science and Insider Threat information session by thanking our representative for joining us today. He really helped us summarize the role Behavioral Science personnel, like himself, play in deterring, detecting, analyzing, and mitigating potential insider threats.

Dr. Atkinson: Thanks. It was a pleasure to be here.

Narrator: We now know that Behavioral Science personnel provide support that is invaluable to Insider Threat Hub teams and greatly benefits risk mitigation efforts.