INSIDER THREAT WEBINAR SERIES

PSYCHOLOGY OF INSIDER THREATS: THE CRITICAL PATHWAY TO AN INSIDER ATTACK
TODAY’S PRESENTATION

• Host: Kelley Easter

• Guest: Kirk Kennedy, Ph.D.
PERSONAL PREDISPOSITIONS
- Mental Health Issues
  - Personality Dysfunction
  - Social Skills Deficits
  - Addictions
  - Poor Judgment
  - Rule-Breaking
  - Competing Identities

STRESSORS
- Personal Professional

CONCERNING BEHAVIORS
- Mental Illness/Addictions/Conflicts
- Deception
- Security/Technical
- Suspicious Travel/Social Networks/Communications

CRIME SCRIPT
- Espionage/Sabotage/Leaks

A PATH TO ESPIONAGE
Case Study: Most Damaging Spy in US History, Robert Hanssen
QUESTIONS?

CONTACT:
Kirk Kennedy, Ph.D.
kkenndey2@fbi.gov

(703) 632-4374
FY20 WEBINAR SCHEDULE

• **March 12** – Industry Insider Threat Programs review and recommendations PERSEREC/Mitre

• **April 30** – OUSD(I) A&A with Josh and Steve

• **June 11** – Insider Threat Lab with PERSEREC

• **August 6** – Table Top Exercise Job Aid Demo

• **September 3** – Insider Threat Awareness Month Virtual Conference
WHAT’S NEW AT CDSE?

Insider Threat Vigilance Campaign 2020

CDSE PRESENTS...
THE CRITICAL PATHWAY

Season Two of the Insider Threat Vigilance Video Series
Each episode helps the workforce understand how to identify and report potential risk indicators.
True Stories from the Inside
Turning people around, not turning them in!

CPR for a troubled mind!

Insider Threat Programs examine concerning behaviors with a multidisciplinary team to deter, detect, and mitigate risks associated with insiders. This proactive strategy often identifies and resolves issues before a potential insider becomes a threat to themselves or protected resources such as personnel, information, and property. Insider Threat Programs can only address these behaviors if they are reported. Many of us feel conflicted about reporting when we notice concerning behavior and worry that we’ll cause problems “over nothing.” However, it’s essential that all concerning behavior be reported. If it’s nothing, no action will be taken. In the cases of increased risk, Insider Threat Programs have an opportunity for intervention prior to any negative event. The goal is to get the help needed, before the situation gets out of control.

The following events are based on a true story.

The Insider Threat office of a U.S. Government agency observed a significant number of agency personnel who were experiencing some type of mental health issues. They observed signs and symptoms of depression, anxiety, psychosis, and in some cases suicidal ideation.

The agency’s Insider Threat – Threat Management Unit (TMU), made up of investigators from the agency’s police force, wanted to do more than just respond to these individuals. They identified an external program taught to both law enforcement personnel and police officers called “Mental Health First Aid” (MHFA). Just as CPR helps you assist an individual having a heart attack, “Mental Health First Aid” helps you assist someone experiencing a mental health or substance use-related crisis. Mental Health First Aid teaches students how to help overcome the stigma of mental health issues, how to identify the physical and behavioral signs and symptoms of mental illness and how to approach and encourage those suffering to seek professional help and treatment.

The TMU members attended the training and were impressed by its content. They became certified instructors themselves.

In the Mental Health First Aid course, participants learn risk factors and warning signs for mental illness, addiction, and suicide concerns, strategies for how to help someone in both crisis and non-crisis situations, and where to turn for help.

Sensor leadership at the agency was asked about the value of having MHFA-trained employees and agreed to the implementation of a MHFA program for their agency.

What were the potential insider threat risk indicators?

- Altered mental health
- Symptoms of depression and anxiety
- Diagnosed psychosis
- Some cases of suicidal ideation

What was the outcome?

- Agency Police Officers and Insider Threat staff are trained in MHFA
- Threat Management Unit conducted numerous training courses to other divisions and supervisors
- Employees were trained to identify co-workers and family members struggling with a mental health crisis and provide a way for early intervention

Volume 2

Introduction

This job aid provides lessons learned from school safety program studies for organization to consider in self-assessment of their insider threat programs’ preparation and response to the threat of kinetic violence. There have been more than 250 active shooter incidents since 2000, with more than 50 of them occurring within the education system in 2012. Studies showed that school size and security posture differ significantly. There is no one-size-fits-all solution, and your program will vary based on the size and complexity of your organization. Factors such as entrance and egress points, physical barriers, on-site law enforcement or security presence; training and awareness, including active shooter drills, and services provided to employees in need of help should be customized to address both threats and vulnerabilities at your location.

Self-Assessment

Organizations should incorporate a self-assessment to evaluate their security posture and the effectiveness of their insider threat program to implement preventive and protective measures to address the risk posed by an active shooter. Self-assessments should be conducted on a continuous basis to properly identify threats and vulnerabilities and work to mitigate associated risks to personnel, facilities, networks, and information, including threats of kinetic violence. Specifically, the inclusion of active shooter drills is recommended.

Lessons learned from school safety

The U.S. Secret Service National Threat Assessment Center’s operational guide is available for public use on the DNI website. This guide provides actionable steps that can be taken to develop comprehensive targeted violence prevention plans for organizations. These lessons trained and recommendations for school safety best practices can be applied to many organizations.

Key considerations

- The threat assessment process is an effective component in ensuring the security and safety of organizations. Organizations should consider the employment of trained threat assessment teams, which are viewed as the best way to prevent violent incidents.
- Threat assessment procedures recognize that employees engage in a continuum of concerning behaviors. The vast majority of these behaviors will be non-threatening and non-violent but may require intervention. Organizations should consider incorporating behavioral science personnel as part of their teams to conduct behavioral threat assessments.
- The threat threshold for intervention may be relatively low, which can help identify employees with concerning behavior in its early stages.
- Threat assessment procedures recognize that employees engage in a continuum of concerning behaviors. The vast majority of these behaviors will be non-threatening and non-violent but may require intervention. Organizations should consider incorporating behavioral science personnel as part of their teams to conduct behavioral threat assessments.
- Everyone has a role to play. Employees should feel empowered to come forward without fear of retaliation. Managers and staff should take all incoming reports seriously and assess...
CDSE INSIDER THREAT SENTRY – MOBILE APPLICATION FOR ANDROID AND IPHONE

Available Soon in iTunes App Store and Google Play
WHERE TO FIND US

https://www.cdse.edu/

http://www.youtube.com/user/dsscdse

http://tinyurl.com/3p6ghle

https://twitter.com/TheCDSE

COMING SOON
Insider Threat Mobile Awareness App
InsiderThreat.Gov