Student Guide

Establishing an Insider Threat Program for Your Organization

Lesson 2: Setting Up an Insider Threat Program

Introduction

Objectives

Insider threat programs as outlined in the national policy and Minimum Standards seek to mitigate the risk of insider threats. This lesson provides guidance on how to set up an insider threat program in your agency or organization.

Program Establishment

Roles and Responsibilities

Each agency must establish its own capability to deter, detect, and respond to the insider threat. This centralized capability relies on several entities. There is a Senior Official who manages the program. In addition, in order to establish the program, key organization stakeholders must be involved. This can be thought of as a working group. Finally, establishing the program also includes putting in place the capability to execute the program. For ease of discussion, we'll describe this as the "hub".

The Senior Official

The Minimum Standards require an agency to designate a Senior Official. The Senior Official plays a vital role in establishing the process of gathering, integrating, analyzing, and responding to potential insider threat information.

When establishing your own insider threat program, it is important to have the buy-in and continuing involvement of your agency's Senior Official. The Senior Official is responsible for managing and overseeing the program and providing resource recommendations to the agency head, submitting the implementation plan and annual reports to the agency head, ensuring proper handling and use of records, consulting with the Office of the General Counsel, civil liberties, and privacy officials; establishing guidelines for record retention; and facilitating oversight reviews to ensure compliance with policy.

Establishing the Working Group

When establishing your agency or organization's capability to deter, detect, and respond to the insider threat, you should establish a working group that includes representatives from key stakeholder offices within your organization. This includes those who can provide personnel-related information, such as counterintelligence, security, and human resources; those who can provide system monitoring, such as information technology and information assurance; those who can provide legal guidance, such as the office of the General Counsel; and, finally, those who can provide response capabilities, such as the Inspector General and law enforcement.

Identifying What Requires Protection

One of the key activities when establishing an insider threat program is to identify and prioritize what requires protection. This may include people, facilities, technology, equipment, and information. However, with limited resources, you cannot protect all assets. Of the assets you do protect, you cannot protect them at the same level.

To help in identifying and prioritizing, ask:

- Is the asset essential for the organization to accomplish its mission?
- Would loss of access to the asset disrupt time-sensitive processes?
- Would compromise or degradation of the asset damage U.S. national or economic security?
- Could an adversary exploit or manipulate this asset to harm the organization, U.S., or allied interests?
- Would an adversary gain advantage by acquiring, compromising, or disrupting the asset?

The answers to these questions will guide you to identify and prioritize what requires protection.

Other Considerations

When establishing the program, other considerations include:

- Who are our key agency stakeholders?
- What resources are available to us?
- What capabilities do we already have in place?
- How should we incorporate subordinate entities?
- How will we apply our program to contractors?

The answers to these questions will guide you in setting up an insider threat program within your organization.

Executing Program Capabilities

Once the insider threat program is established in your organization, there needs to be a centralized capability in place to execute the program. This centralized capability can be thought of as a hub.

Hub activities include:

- Accessing agency-internal information to detect and/or analyze potential insider threats.
- Receiving insider threat reports from inside the agency.
- Developing informed responses to insider threat activity.

Review Activity

Which of the following stakeholders should be involved in establishing an insider threat program in an agency?

Select all that apply.

- ☐ Information Assurance
- ☐ Security
- ☐ Human Resources
- ☐ Research and Development

Answer Key

Review Activity

Which of the following stakeholders should be involved in establishing an insider threat program in an agency?

Select all that apply.

- ☑ Information Assurance
- ☑ Security
- ☑ Human Resources
- ☐ Research and Development

Information Assurance, Security, and Human Resources are just a few of the stakeholders that should be included.