Student Guide

Establishing an Insider Threat Program for Your Organization

Lesson 1: Insider Threat Program Requirement

Introduction

Objectives

Who could become an insider threat? An insider is any person with authorized access to any United States government resource, such as personnel, facilities, information, equipment, networks or systems. An insider threat refers to an insider who wittingly or unwittingly does harm to the security of the United States. This threat can include espionage, terrorism, sabotage, unauthorized disclosure of national security information, or the loss or degradation of departmental resources or capabilities. Insider threat programs seek to mitigate the risk of insider threats.

This lesson will review program policies and standards. It will also discuss the key challenges to detecting insider threats.

Regulatory Framework

Background

We are all too familiar with the most notorious of insider threat cases. In response to the threat from insiders, national policy issued in late 2011 requires government agencies to establish insider threat programs. For now, this policy applies only to classified information, though its principles can help you protect all of your organization's information. Let's take a closer look at the policy and its requirements.

National Policy

Executive Order 13587 establishes the requirement for government agencies to establish their own insider threat programs. The Order defines the insider threat program purpose as deterring, detecting, and mitigating insider threats.

Insider threat programs are intended to: Deter cleared employees from becoming insider threats; detect insiders who pose a risk to classified information; and mitigate the risks through administrative, investigative, and other response actions.

The Executive Order also includes general department and agency responsibilities that we will discuss throughout this course.

General Department and Agency Responsibilities

- Within 180 days of the effective date of this policy (May 20, 2013), establish a program for deterring, detecting, and mitigating insider threat; leveraging counterintelligence (CI), security, information assurance, and other relevant functions and resources to identify and counter the insider threat.

- Establish a centralized capability to monitor, audit, gather and analyze information for insider threat detection and mitigation. Critical program requirements include but are not limited to: (1) monitoring user activity on classified computer networks controlled by the Federal Government; (2) evaluation of personnel security information; (3) employee awareness training of the insider threat and employees' reporting responsibilities; and (4) information analysis, reporting, and response capability.

- Develop and implement sharing policies and procedures whereby the organization's insider threat program accesses, shares, and integrates information and data derived from offices across the organization, including CI, security, information assurance, and human resources offices.

- Designate a senior official(s) with authority to provide management, accountability, and oversight of the organization's insider threat program and make resource recommendations to the appropriate agency official.

- Consult with records management, legal counsel, and civil liberties and privacy officials to ensure any legal, privacy, civil rights, civil liberties issues (including use of personally identifiable information) are appropriately addressed.

- Promulgate additional department/agency guidance, if needed, to reflect unique mission requirements but not inhibit meeting the minimum standards issued by the Insider Threat Task Force (ITTF) pursuant to this policy.

- Perform self-assessments of compliance with insider threat policies and standards; the results of which shall be reported to the Senior Information Sharing and Safeguarding Steering Committee (hereinafter Steering Committee).

- Enable independent assessments, in accordance with Section 2.1(d) of EO 13587, of compliance with established insider threat policy and standards by providing information and access to personnel of the Insider Threat Task Force (ITTF).

Minimum Standards

In November 2012, the Executive Branch issued Minimum Standards for Executive Branch Insider Threat Programs. Issued in the form of a Presidential Memorandum, these standards outline the minimum requirements to which all executive branch agencies must adhere. These elements include the capability to gather, integrate, centrally analyze, and respond to key threat-related information; monitor employee use of classified networks; provide the workforce with insider threat awareness training; and protect the civil liberties and privacy of all personnel.

While the Minimum Standards provide the minimum elements needed for agencies to establish effective insider threat programs, agencies may go farther, if they choose.

Throughout this course, we will examine these minimum requirements in greater detail.

Challenges to Detecting the Insider Threat

Why Do Insiders Go Undetected?

The reason why the Executive Branch issued the insider threat national policy and minimum standards is that it is often difficult to identify insiders who pose a threat and to detect what they are doing in time to prevent harm. Insiders can operate over an extended period of time. Employees may not be trained to recognize reportable suspicious activity or may not know how to report, and even when employees do recognize suspicious behaviors, they may be reluctant to report their co-workers. It is also important to note that the unwitting insider threat can be as much a threat as the malicious insider threat. Traditional access controls don't help – insiders already have access. Insiders can collect data from multiple systems and can tamper with logs and other audit controls. It is difficult to distinguish malicious from legitimate transactions.

Insider threat program requirements are designed to help address these challenges.

Review Activity 1

The minimum standards for establishing an insider threat program include which of the following?

Select the best responses.

- ☐ Establish capability to manage threat information
- ☐ Monitor employee classified network use
- ☐ Provide employee training
- ☐ Protect civil liberties and privacy

Review Activity 2

What is an insider threat?

Select the best response.

- ○ An insider threat is a threat that a person with access to any United States government resources will use his or her access to wittingly do harm to the security of the U.S.
- ○ An insider threat is a threat that a person with authorized access to any United States government resources will use his or her access, wittingly or unwittingly, to do harm to the security of the U.S.

Answer Key

Review Activity 1

The minimum standards for establishing an insider threat program include which of the following?

Select the best responses.

- ☑ Establish capability to manage threat information
- ☑ Monitor employee classified network use
- ☑ Provide employee training
- ☑ Protect civil liberties and privacy

All of these are included in the minimum standards for establishing an insider threat program.

Review Activity 2

What is an insider threat?

Select the best response.

- ○ An insider threat is a threat that a person with access to any United States government resources will use his or her access to wittingly do harm to the security of the U.S.
- ⊙ An insider threat is a threat that a person with authorized access to any United States government resources will use his or her access, wittingly or unwittingly, to do harm to the security of the U.S.

It is important to remember that insider threats can be both witting and unwitting.