Risk Management for DoD Security Programs Training

Glossary

Adversary

An adversary is any individual, group, organization or government that conducts activities, or has the intention and capability to conduct activities detrimental to critical assets.

Asset

An asset is anything of value or importance to the organization or an adversary, such as people, computers, buildings or strategic advantages. The nature and magnitude of that value may differ.

Capability

Capability refers to an adversary's ability or capacity to act as a potential threat to an asset.

Countermeasure

Countermeasures are actions of any type used to reduce or eliminate one or more vulnerabilities.

Covert

An operation planned and executed to conceal the identity of, or permit plausible denial by, the sponsor. A covert operation is similar to law enforcement's undercover operation.

Criminal

A criminal is an adversary who violates the law causing the loss of or damage to assets. Examples include violent acts against people, theft, hacking, etc.

Economic espionage

Economic espionage is the theft or misappropriation of U.S. proprietary information or trade secrets, especially to foreign governments and their agents. Both traditionally friendly nations and recognized adversaries conduct economic espionage.

Foreign industrial espionage

Foreign industrial espionage is industrial espionage conducted by a foreign government or a foreign company with direct assistance of a foreign government against a private U.S. company for the purpose of obtaining commercial secrets.

Foreign intelligence entity

Foreign intelligence entities refer to an organization that is part of a foreign government and engages in intelligence activities.

Goals

Adversary goals may include gaining attention, exacting revenge, living better, capturing market share, making money, and furthering political, economic, military, ethnic or religious agendas.

HUMINT

HUMINT, the acronym for human intelligence, is intelligence derived from people through interviews, elicitation, or reports originating from people.

History

History is an account of past actions taken against assets.

IMINT

The acronym for imagery intelligence, involves using various sources, such as satellites, photos, infrared, imaging radar, and electro-optical, for collecting image data.

Impact

An impact is the amount of loss or damage that can be expected from a successful asset attack or other undesirable event. Loss may be monetary but may also include political, moral, and operational effectiveness impacts.

Insider

An insider is an adversary who has special access or privileges. Examples include employees, contractors, customers, etc.

Intent

Intent refers to an adversary's future or intended plans that may pose a threat to an asset. Analyzing intent requires an understanding of the adversary's perspective.

Linguistic value

The linguistic values are critical (C), high (H), medium (M), and low (L).

MASINT

MASINT is the acronym for measurement and signatures intelligence. It excludes signals intelligence and traditional imagery intelligence. When collected, processed, and analyzed, MASINT locates, tracks, identifies, or describes the signatures (distinctive characteristics) of fixed or dynamic target sources. It includes the advanced data processing and exploitation of data from overhead and airborne imagery collection systems. MASINT data can be acquired from a variety of satellite, airborne, or ship borne platforms; remotely piloted vehicles; or from mobile or fixed ground-based collection sites.

National-level security policy initiatives

National-level security policy initiatives include the Joint Security Commission Report (1994), the Presidential Decision Directive/PDD-29, and the National Security Council/Security Policy Board Risk Management Strategy.

Natural disasters

Natural disasters are phenomena that occur in nature that have the potential to damage assets or interrupt activities and operations. Examples include floods, lightning, tornadoes, volcanic eruptions, etc.

Need to know

Need to know is a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

Numerical rating

Numerical ratings are used to allow for a more precise rating. The numerical ratings generally range on a scale of 1 to 100.

OSINT

OSINT, the acronym for open source intelligence, includes resources such as newspapers, internet, magazines, international conventions, Freedom of Information Act (FOIA) requests, seminars, and exhibits, e.g. CNN.com, The New York Times, and Space & Technology.

Overt

Overt describes an operation conducted openly to acquire information via the public domain.

Regressive analysis

Regressive analysis is the five-step process for analyzing the asset in an unprotected state first and then analyzing the asset in conjunction with current countermeasures.

Risk management (RM)

Risk management is the process of selecting and implementing countermeasures to achieve an acceptable level of risk at an acceptable cost.

Risk

A risk is the potential for damage to or loss of an asset.

SIGINT

SIGINT, the acronym for signals intelligence, is comprised of communications and the electronic and telemetry collection of information in the non-visible portion of the electromagnetic spectrum.

Terrorist

A terrorist is an adversary who uses violence or the threat of violence to inculcate fear with the intent to coerce or intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. Examples include Al Qaeda, HAMAS, etc.

Threat

A threat is any indication, circumstance, or event with the potential to cause the loss of or damage to an asset. Threat may also be defined as the intention and capability of an adversary to act detrimentally to an asset owner's interests.

Undesirable events

AAn undesirable event is an event/action that adversely affects an asset. Common undesirable events toward an asset include unauthorized entry, terrorist bombing, unauthorized access to sensitive computer files, and loss of classified documents. Natural disasters and accidents, such as flood, fire, or high winds, may also be considered, of course, an undesirable event.

Vulnerabilities

A vulnerability is any weakness that can be exploited by an adversary to gain access to or information from an asset. Vulnerabilities can be evident in building characteristics; equipment properties, personal behavior, locations of people, and operational and personnel practices.