CTSC Operational Glossary of Cybersecurity Terms

v1.0

About this document:

This glossary consists of operational definitions of key terms used in CTSC cybersecurity activities, including risk assessments and broader risk management activities. Wherever possible we have selected definitions from other authorities (*e.g.*, FISMA, NIST Standards) as the basis for CTSC's operational definitions. Where necessary, definitions have been customized to clarify the interrelatedness of terms and increase their relevance to the communities we serve. **Bold, red** emphasis notes terms that are defined elsewhere in this glossary. A primary goal of this glossary is to support clarity and internal consistency in our usage. This glossary will be revised and updated on a rolling basis as warranted. Notes following definitions are designed to aid clarity and incorporate guidance for usage.

Contents

Asset

Assets are valuable and/or **sensitive** organizational **information** and **information systems**.

Notes:

1. Assets have a basic level of organizational *value* and/or *sensitivity* that can be estimated (*e.g.*, as high, medium, low). This value/sensitivity level is just one factor worth considering in analyzing the anticipated impact of security incidents. See, **Impact, Estimation of**.
2. We distinguish assets from the broader organizational interests (*e.g.,* property, operations, reputation/goodwill, safety and well-being of individuals, other organizations and stakeholders) that cybersecurity efforts assist in protecting.
3. We employ an asset/impact-oriented analysis as a default for risk assessments, and particularly when assisting entities with broad (*e.g.*, full cybersecurity program scale) planning. See the definition of **Risk Assessment** for more.
4. In practice, our risk assessment and management work often focuses on assets with significant value and/or sensitivity levels (*e.g.*, information systems critical to the science mission of a project).
5. To give practical advice, we often must define specific assets at various levels of abstraction. Probably all engagee projects have IT infrastructure as an asset, and we may be able to give broad advice regarding securing IT infrastructure. At the same time, many engaged communities will have some very specific and unique assets warranting closer analysis (*e.g.*, a special instrument array; a specific data set).
6. We use “assets” or “information assets” interchangeably.

Attack Surface

Attack surfaces are the portions or components of an **information system** through which the unauthorized access, use, disclosure, disruption, modification, or destruction of information **assets** may take place.

Notes:

1. A single **asset** (*e.g.*, raw research data collected by a specialized instrument) may be susceptible to attack via multiple surfaces.
2. We use “attack surface” and “surface” interchangeably.

Cybersecurity Plan

A cybersecurity plan is a document or set of documents outlining a **cybersecurity program** or other organized approach to addressing information security risks to an entity.

Cybersecurity Program

A cybersecurity program is a structured approach to develop, implement and maintain an organizational environment conducive to appropriate information security and levels of information-related risk. Cybersecurity programs entail ongoing activities to address relevant policies and procedures; technology and mitigations; and training and awareness [2] [10]. Cybersecurity programs are scoped to the key assets, resources, and lifespan of organizations.

Impact, Estimation of

Impact refers to the estimated magnitude of harm to organizational interests (*e.g.,* property, operations, reputation/goodwill, safety and well-being of individuals, other organizations and stakeholders) due to a loss of information security.

Notes:

1. In performing risk assessments, we estimate the impact of adverse events, generally categorizing impact levels as High (Severe/Catastrophic), Moderate (Serious), and Low (Limited) [4].
2. In estimating impact, the following factors should be considered where applicable:
    a. Asset value
    b. Asset **sensitivity**
    c. Nature of the interest and type of resultant harm flowing from a loss of confidentiality, integrity, and/or availability (*e.g.*, loss of human life, damage to reputation, inconvenience to end users)
    d. Scope of resultant harm across time (including length of time), and number and type of stakeholders
    e. Effectiveness of any existing detective and responsive mitigations
    f. The knowledge, confidence and expertise of the those performing the estimation

Incident

A security incident is a **threat** that has manifested itself in such a way as to warrant a response due to an imminent or actual **loss of information security**.

Information

Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual [3].

Information Security, Loss of

The term information security means protecting information **assets** from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide for the information security objectives of confidentiality, integrity, and availability [1]. "A loss of information security" is synonymous with the "unauthorized access, use, disclosure, disruption, modification, or destruction of information assets."

Confidentiality

Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information [1]. A loss of confidentiality is the unauthorized disclosure of **information** [4].

Integrity

Guarding against improper information modification or destruction, and includes ensuring information authenticity [1]. A loss of integrity includes the unauthorized modification or destruction of **information** [4], and the unauthorized control of an **information system**.

Availability
Ensuring timely and reliable access to and use of **assets** [1]. A loss of availability is the disruption of access to or use of an asset [4].

Information System

An information system is a discrete set of information and related resources (such as people, equipment, and information technology) organized for the collection, processing, maintenance, use, sharing, dissemination, and/or disposition of **information** [5].

Notes:

1. For risk assessment purposes, information systems may be treated as **assets**, but also may be containers for assets (*e.g.*, sensitive/valuable information).
2. The term "discrete" in this definition is not meant to imply that information systems always have precisely definable boundaries. Often, we must impose this discreteness with pragmatic system characterizations. Sometimes this means carving out smaller information systems that exist within larger information systems.

Likelihood, Estimation of

Likelihood is an estimation of the probability of the occurrence of a security **incident**.

Notes:

1. In performing risk assessments, we estimate the likelihood of incidents occurring, generally categorizing likelihood levels as High, Moderate, and Low. In estimating likelihood, the following factors should be considered where applicable:
    a. Motivation, knowledge, and capabilities of potential threat sources
    b. Specifics of any relevant **vulnerability**
    c. Effectiveness of existing preventative **mitigations**
    d. Anticipated frequency of the adverse event occurring
    e. The knowledge, confidence and expertise of the those performing the estimation
2. While historical evidence and experience help, estimating likelihood is a very subjective activity.
3. Note that likelihood estimations relate to the likelihood of incidents. Incidents include events where there is an imminent or actual loss of information security. Therefore, incidents and likelihood estimations encompass a range of events, from successful, harmful attacks to attempts or near-misses where response is warranted.

Mitigations

Mitigations are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and/or availability of information **assets** [6].

Notes:

1. Mitigations are employed to *prevent*, *detect*, *respond to*, and *recover from* security incidents. They are employed to reduce the likelihood and/or impact of incidents.

2. We use “controls” and “mitigations” more-or-less interchangeably. While “controls” may imply technical safeguards and countermeasures, we believe “mitigations” better captures the full, broad range of safeguards and countermeasures.

Risk Level

Risk level is a measure of the extent to which an entity is threatened by a potential security **incident**. Risk level is a function of: (i) the estimated **likelihood** of a threat manifesting itself as an **incident**; and (ii) the estimated **impact** of the **incident**. [7]

Notes:

1. In common usage, “risk” is often used to describe the likelihood of some event occurring (*e.g.*, “there is a high *risk* of a tornado touching down”). This is not our usage.
2. “Risk” is also often used to refer to what we define here as a “threat,” *i.e.*, a circumstance or event with the potential to adversely impact an entity.

Risk Assessment

Risk assessments are used to identify, estimate, and organize threats to an entity. Their purpose is to inform decision makers and support broader risk management processes. Risk assessments can vary both in assessment approach (*e.g.*, qualitative, semi-quantitative) and orientation or starting point (*e.g.*, asset/impact-oriented analysis, vulnerability-oriented analysis) [7].

Notes:

1. The results of a risk assessment are typically used to guide the selection and deployment of **mitigations**.
2. We have employed both asset/impact-oriented and vulnerability-oriented analyses in carrying out cybersecurity risk assessments. See the definitions for **asset** and **vulnerability**.

Risk Management

Risk management refers to a coordinated set of activities and methods that is used to direct an organization and to understand and respond to the many **threats** that can affect its ability to achieve its objectives [8]. Ongoing risk management activities are typically a substantial component of a cybersecurity program. Cybersecurity planning and programs are often components of broader risk management activities within an organization.

Sensitive

Sensitive describes information and information systems for which unauthorized access, use, disclosure, disruption, modification, or destruction could negatively impact organizational operations, organizational assets, individuals, other organizations or stakeholders.

Notes:

1. Many organizational assets are both valuable and sensitive; these terms are not mutually exclusive. Used together, these terms capture the scope of an organization’s basis for utilizing resources to protect information assets.

Threat

Any circumstance or event with the potential to adversely **impact** organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations and/or stakeholders through an **information system** via a **loss of information security** [9].

Notes:

1. Cybersecurity threats often can be described at various levels of abstraction or granularity. In practice, we work to describe threats at a level of detail which best assists engaged parties in making risk management decisions, *e.g.*, recommending **mitigations** to give the most return on investment of limited resources.
2. Threats often can be described in terms of a threat source (*e.g.*, an actor) and the action taken. For example, *an employee inappropriately shares sensitive communications*.
3. Threats include potential circumstances or events resulting from accidental, negligent and reckless actions, as well as malicious actions.

Vulnerability

A vulnerability is a weakness in an information system that warrants **mitigation** [3].

Notes:

1. Some cybersecurity risk assessment approaches suggest that a threat always maps to a vulnerability. Our approach is less constrained, and accounts for **attack surfaces** that may not be fairly described as "weaknesses" or "gaps."
2. A vulnerability-oriented **risk assessment** or vulnerability assessment, when employed, focuses primarily on identifying security weaknesses in information systems that warrant mitigation [7].

* * *

References

[1] *See*, 44 U.S.C. 3542(b)

[2] Based on a definition provided by James Marsteller.

[3] *National Information Assurance (IA) Glossary,* CNSS Instruction No. 4009, Apr. 2010.

[4] *Standards for Security Categorization of Federal Information and Information Systems,* FIPS Publication 199, Feb. 2004.

[5] *See*, 44 U.S.C. 3502

[6] *Standards for Security Categorization of Federal Information and Information Systems,* FIPS Publication 199, definition of "security controls", Feb. 2004.

[7] *Guideline for Conducting Risk Assessments,* NIST Special Publication 800-30 Revision 1, Sept. 2012.

[8] *See*, Praxiom Research Group Limited (2010, Aug. 31). "Risk Management Dictionary". ISO 31000 [Online]. Available: http://www.praxiom.com/iso-31000-terms.htm.[Accessed: Sept. 17,2013]

[9] *Security and Privacy Controls for Federal Information Systems and Organizations,* NIST Special Publication 800-53 Revision 4, Apr. 2013.

[10] *See, e.g.,* National Science Foundation (NSF) Cooperative Agreement, Supplemental Financial & Administrative Terms and Conditions for Managers of Large Facilities, Effective February 1, 2012, Article 56, Information Security.