

OCTAVE^{SM*} Threat Profiles

Christopher Alberts and Audrey Dorofee
Software Engineering Institute
Carnegie Mellon University

The Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVESM) is an information security risk evaluation that is comprehensive, systematic, and context driven [1]. By following the OCTAVE Method, an organization can make information-protection decisions based on risks to the confidentiality, integrity, and availability of critical information technology (IT) assets. The operational or business units and the IT department work together to address the information security needs of the organization. In this paper, we focus on how to document the threats to the organization's critical assets by creating a threat profile.

1.0 Background

Using a three-phase approach, OCTAVE examines organizational and technology issues to assemble a comprehensive picture of the information security needs of an organization. The phases of OCTAVE are

- **Phase 1: Build Asset-Based Threat Profiles** – This is an organizational evaluation. Staff members within the organization identify important information assets, the threats to those assets, and the security requirements of the assets. They determine what the organization is currently doing to protect its information assets (protection strategy practices) and identify weaknesses in organizational policies and practice (organizational vulnerabilities).
- **Phase 2: Identify Infrastructure Vulnerabilities** – This is an evaluation of the information infrastructure. The key operational components of the information technology infrastructure are identified based on the information gathered during Phase 1 and then examined for weaknesses (technology vulnerabilities) that can lead to unauthorized action.
- **Phase 3: Develop Security Strategy and Plans** – Risks are analyzed in this phase. The information generated by the organizational and information infrastructure evaluations (Phases 1 and 2) are analyzed to identify risks to the organization and to evaluate the risks based on their impact to the organization's mission. In addition, a protection strategy for the organization and mitigation plans addressing the highest priority risks are developed.

The OCTAVE Method is self directed. A small team of the organization's personnel (called the analysis team) manages the process and analyzes all information. The analysis team is an interdisciplinary team comprising representatives from both the business lines and the IT department of the organization.

2.0 Threat Profile

A key aspect of OCTAVE is the identification and analysis of threats to the organization's assets. A threat is an indication of a potential undesirable event [2]. It refers to a situation in which a person could do something undesirable (an attacker initiating a denial-of-service attack against an organization's email

* Operationally Critical Threat, Asset, and Vulnerability Evaluation and OCTAVE are service marks of Carnegie Mellon University.

server) or a natural occurrence could cause an undesirable outcome (a fire damaging an organization's information technology hardware). Threats consist of the following properties:

- asset – something of value to the organization (information in electronic or physical form, information systems, a group of people with unique expertise)
- actor – who or what may violate the security requirements (confidentiality, integrity, availability) of an asset. Actors can be from inside or outside the organization.
- motive (optional) – indication of whether the actor's intentions are deliberate or accidental
- access (optional) – how the asset will be accessed by the actor (network access, physical access)
- outcome – the immediate result of violating the security requirements of an asset (disclosure, modification, destruction, loss, interruption)

In the OCTAVE Method, the analysis team creates threat scenarios based on known sources of threat and typical threat outcomes. Threats with a common theme can be grouped together. During OCTAVE, the following standard categories of threat are considered:

- human actors using network access – The threats in this category are network-based threats to an organization's critical assets. They require direct action by a person and can be deliberate or accidental in nature.
- human actors using physical access – The threats in this category are physical threats to an organization's critical assets. They require direct action by a person and can be deliberate or accidental in nature.
- system problems – The threats in this category are problems with an organization's information technology systems. Examples include hardware defects, software defects, unavailability of related enterprise systems, viruses, malicious code, and other system-related problems.
- other problems – The threats in this category are problems or situations that are outside the control of an organization. This category of threats includes natural disasters (such as floods, earthquakes, and storms) that can affect an organization's information technology systems as well as interdependency risks. Interdependency risks include the unavailability of critical infrastructures (telecommunications, electricity, etc.). Other types of threats outside the control of an organization can also be included here. Examples of these threats are power outages, broken water pipes, etc.

An organization usually has some control over humans accessing assets over a computer network or by physical means, as well as some control over system problems. The category of other problems is used for those that tend to fall outside the control of the organization. In this category, the effects of the threat can be controlled to some extent, but the source of the threat cannot be controlled.

The resulting outcome or effect of these threat scenarios typically falls into these categories:

- disclosure or viewing of sensitive information
- modification of important or sensitive information
- destruction or loss of important information, hardware, or software
- interruption of access to important information, software, applications, or services

2.1 Visual Representation of the Generic Threat Profile

At the end of Phase 1, the analysis team selects the most critical assets to the organization and creates a threat profile for each critical asset. The range of threats to be considered during the evaluation can be represented visually in tree structures; there is one tree structure for each category of threat (as listed in Section 2.0). Collectively, the set of tree structures is called the generic threat profile. Figures 1-4 show the generic threat profile used during OCTAVE. Note that the trees of the generic threat profile are built around the properties of threats.

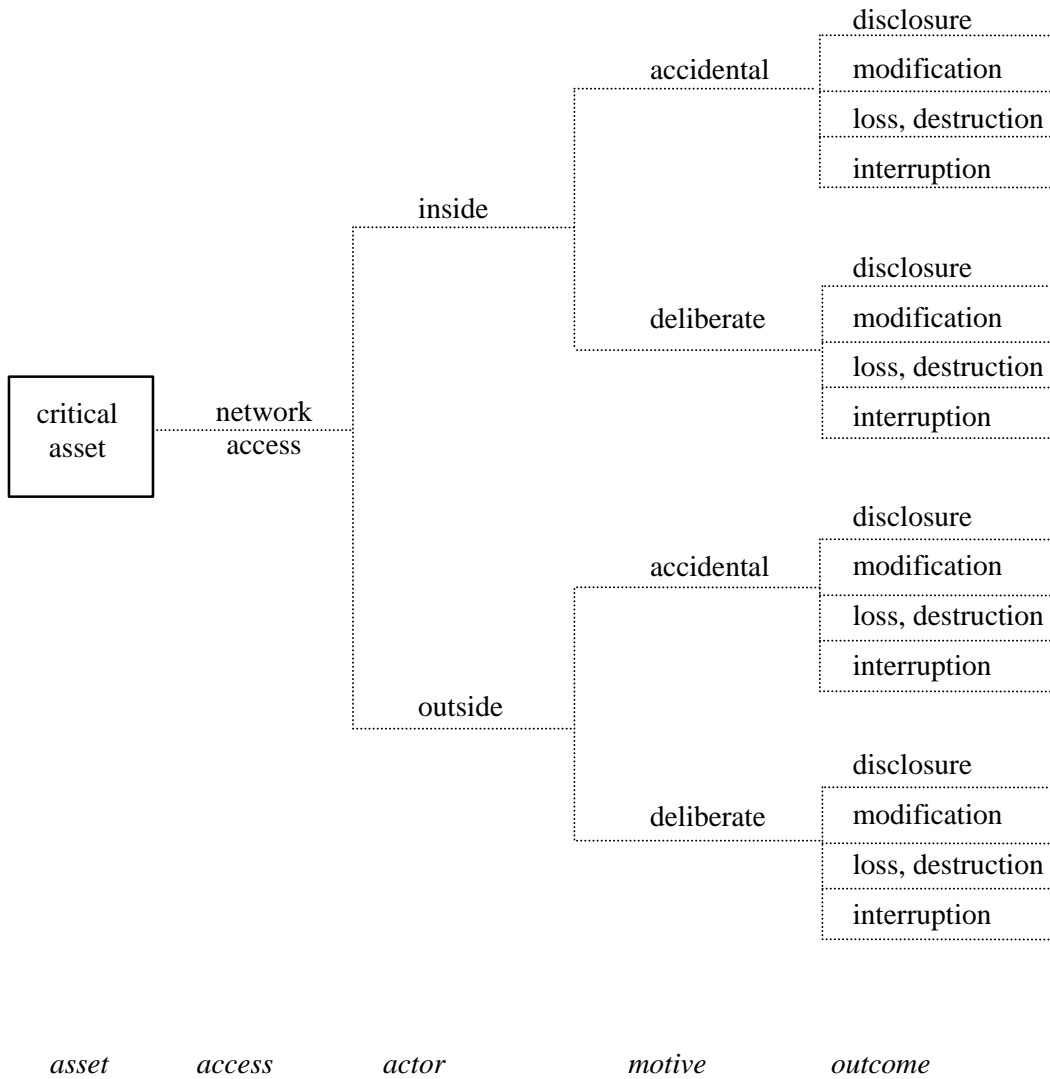


Figure 1. *Human Actors Using Network Access*

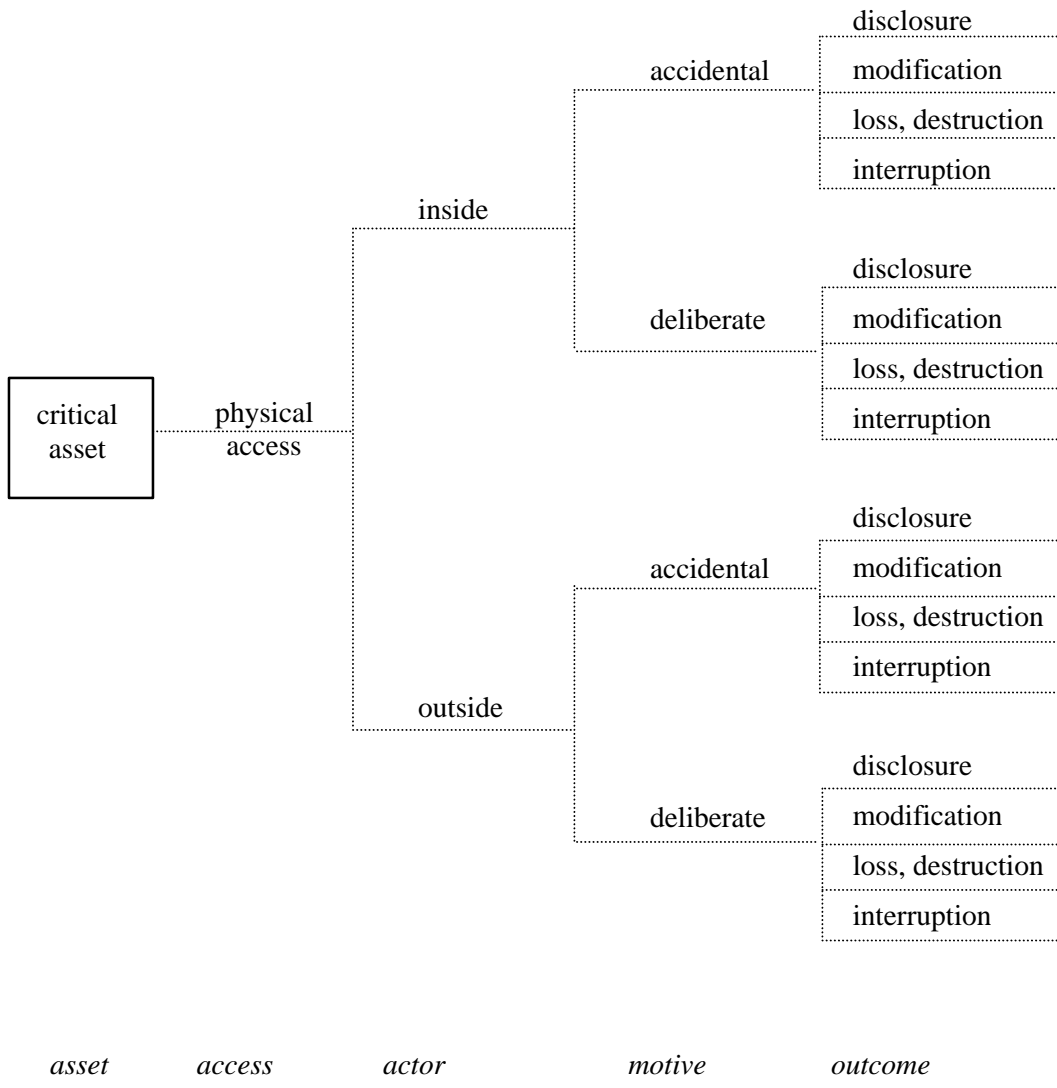


Figure 2. Human Actors Using Physical Access

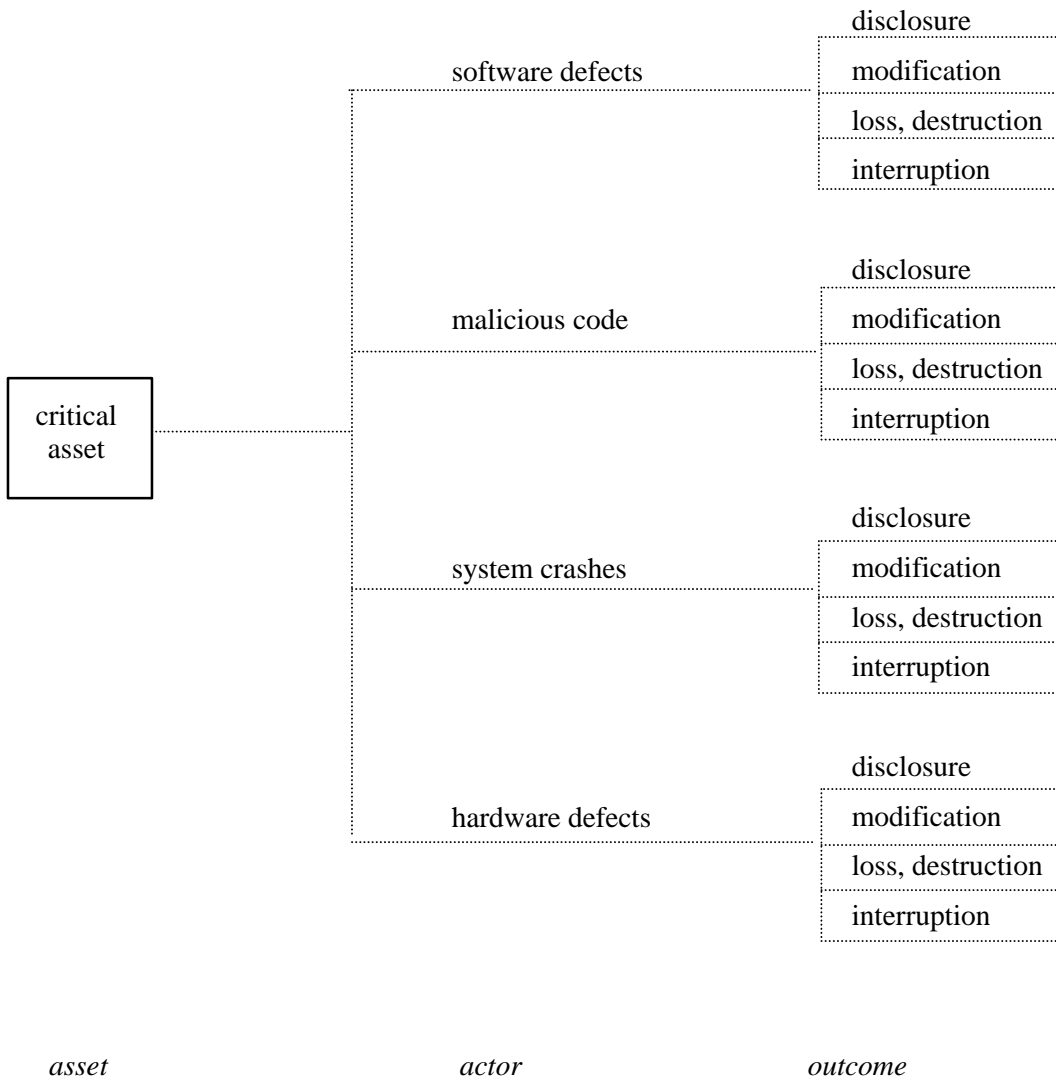


Figure 3. System Problems

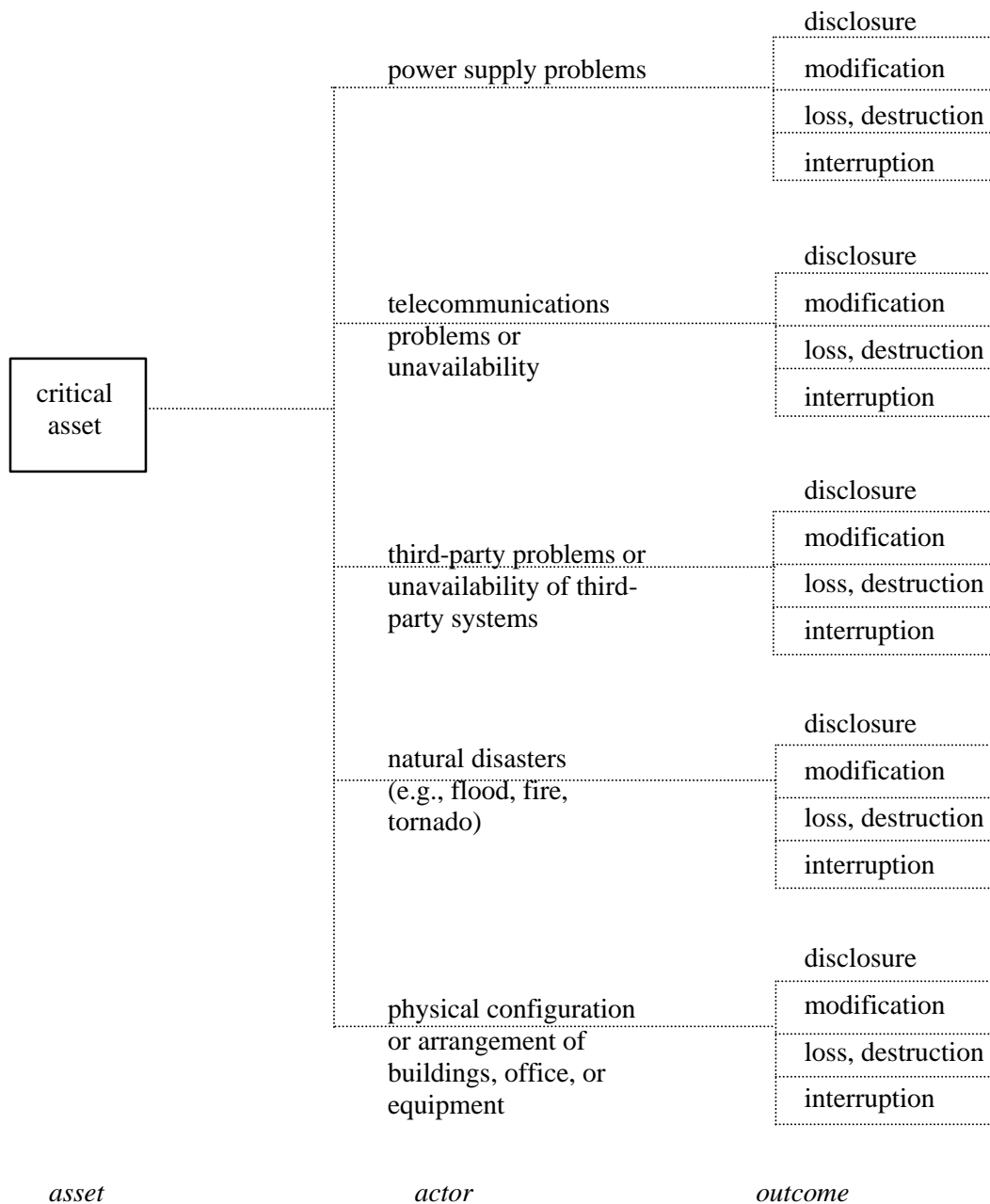


Figure 4. Other Problems

2.2 Extending and Tailoring the Generic Threat Profile

The generic threat profile addresses a standard range of threats to critical assets. Prior to the evaluation, it can be tailored to meet the organization's needs. When tailoring the generic threat profile, the analysis team can

- add a new threat category
- add new threats to an existing category
- delete inapplicable threats from a category
- “decompose” or add depth to a threat category

For some organizations, the standard categories are sufficient. Other organizations might require additional categories of threat. The categories of threat are contextual and are based on the environment in which an organization must operate. The standard categories are a good starting place. As an organization implements OCTAVE, it will start identifying many unique threats. The unique threats might belong in one of the standard categories, or they might require the creation of new categories. In general, the threat profile should be as complete as necessary and should contain no duplication.

The following example addresses tailoring of the threat actors for the *Human Actors Using Network Access* category of threat. The basic threat tree for this category focuses on two types of threat actors: actors inside the organization and actors outside the organization. Depending on the evaluation needs of an organization, this classification of actors could be too broad. An organization that deals with national security issues would probably want a more detailed classification of threat actors. Below is an expanded classification of threat actors.¹

- non-malicious employees – people within the organization who accidentally abuse or misuse computer systems and their information
- disgruntled employees – people within the organization who deliberately abuse or misuse computer systems and their information
- attackers – people who attack computer systems for challenge, status, or thrill
- spies – people who attack computer systems for political gain
- terrorists – people who attack computer systems to cause fear for political gain
- competitors – people who attack computer systems for economic gain
- criminals – people who attack computer systems for personal financial gain
- vandals – people who attack computer systems to cause damage

The asset-based threat tree could be modified to include the above classifications and more detailed motives. In addition, other forms of tailoring can be applied to add detail to the access paths. Furthermore, separate trees could be created for different means of network access or for different means of physical access. The trees will become complicated with the additional detail and could make the subsequent analysis more complex. For most organizations, however, the standard trees will be sufficient for their evaluation needs.

¹ This list was created using references [3], [4], and [5].

3.0 Creating and Using the Threat Profile

During Phase 1 of OCTAVE, the analysis team elicits information from the organization's staff during a series of workshops. This information is used to build the threat profiles for the organization's critical assets. Threat profiles for critical assets are used during Phase 2 when the analysis team identifies key infrastructure components and during Phase 3 when the analysis team identifies and analyzes risks. Thus, the threat profiles for critical assets form the basis for the analysis activities of OCTAVE.

3.1 Gathering Threat Information

Early in Phase 1, the analysis team facilitates knowledge elicitation workshops with staff from multiple organizational levels (senior management, operational area management, and staff). The purpose of the knowledge elicitation workshops is to identify the following information from each organizational perspective:

- important assets and their relative values
- areas of concern (perceived threats to the assets)
- security requirements
- current protection strategy practices
- organizational vulnerabilities

The areas of concern directly relate to the threat profile. Areas of concern are plausible scenarios constructed by the workshop participants that outline concerns about the threats to important assets. The areas of concern are likely to lack sufficient detail with respect to the components of threat, and they are further examined when creating the threat profile for a critical asset.

3.2 Creating a Threat Profile for a Critical Asset

At the end of Phase 1, the analysis team

- groups the information previously elicited from the different organizational levels
- selects critical assets
- creates a threat profile for each critical asset

When creating a threat profile for a critical asset, the analysis team first maps the areas of concern for the critical asset to the generic threat profile. The team then performs a gap analysis to determine if any other potential threats from the profile also apply to the critical asset. This can be shown with an example.

For the example, let us say that an organization has identified the records on system XYZ as a critical asset. Consider the following areas of concern that might have been identified during the first few steps of OCTAVE:

- People are accidentally entering the wrong data into system XYZ. This results in incorrect records on that system.
- Someone could use the records from system XYZ for personal gain.
- Inherent flaws and vulnerabilities in system XYZ could be exploited by attackers to view or change critical information in the records.

Note that each of the above threats is from the *Human Actors Using Network Access* category. Normally, workshop participants identify areas of concern for more than one category of threat. In this example, we

will explore only one category for simplicity. The properties of threat for each area of concern are shown in Table 1:

Area of Concern	Threat Properties
<p>1. People are accidentally entering the wrong data into system XYZ. This results in incorrect records on that system.</p>	<ul style="list-style-type: none"> • asset – system XYZ records • access – network (The data are entered into records on a system.) • actor – insiders (The concern implies staff with legitimate access.) • motive – accidental • outcome – modification (The data are incorrect; they have modified it.)
<p>2. Someone could use the records from system XYZ for personal gain.</p>	<ul style="list-style-type: none"> • asset – system XYZ records • access – network (The actor gets the records from the system.) • actor – insiders and outsiders (The concern implies staff with legitimate access as well as outsiders.) • motive – deliberate • outcome – disclosure (The actor is viewing information that he/she shouldn't be viewing.)
<p>3. Inherent flaws and vulnerabilities in system XYZ could be exploited by attackers to view or change critical information in the records.</p>	<ul style="list-style-type: none"> • asset – system XYZ records • access – network (The actor gets the records from the system.) • actor – outside (The concern states that the actors are “attackers.”) • motive – deliberate • outcome – disclosure, modification

Table 1. Threat Properties for Areas of Concern

Now that the threat properties of each area of concern have been identified, the analysis team can easily map the threat properties to the generic threat profile. Notice that an area of concern can be ambiguous. In this case, the analysis team must use its judgment when identifying the threat properties. For example, in the second area of concern in the table, the threat actor is stated as “someone.” The analysis team

interpreted this to mean both insiders and outsiders. The following diagram shows the mapping of the areas of concern to the threat tree for *Human Actors Using Network Access*.

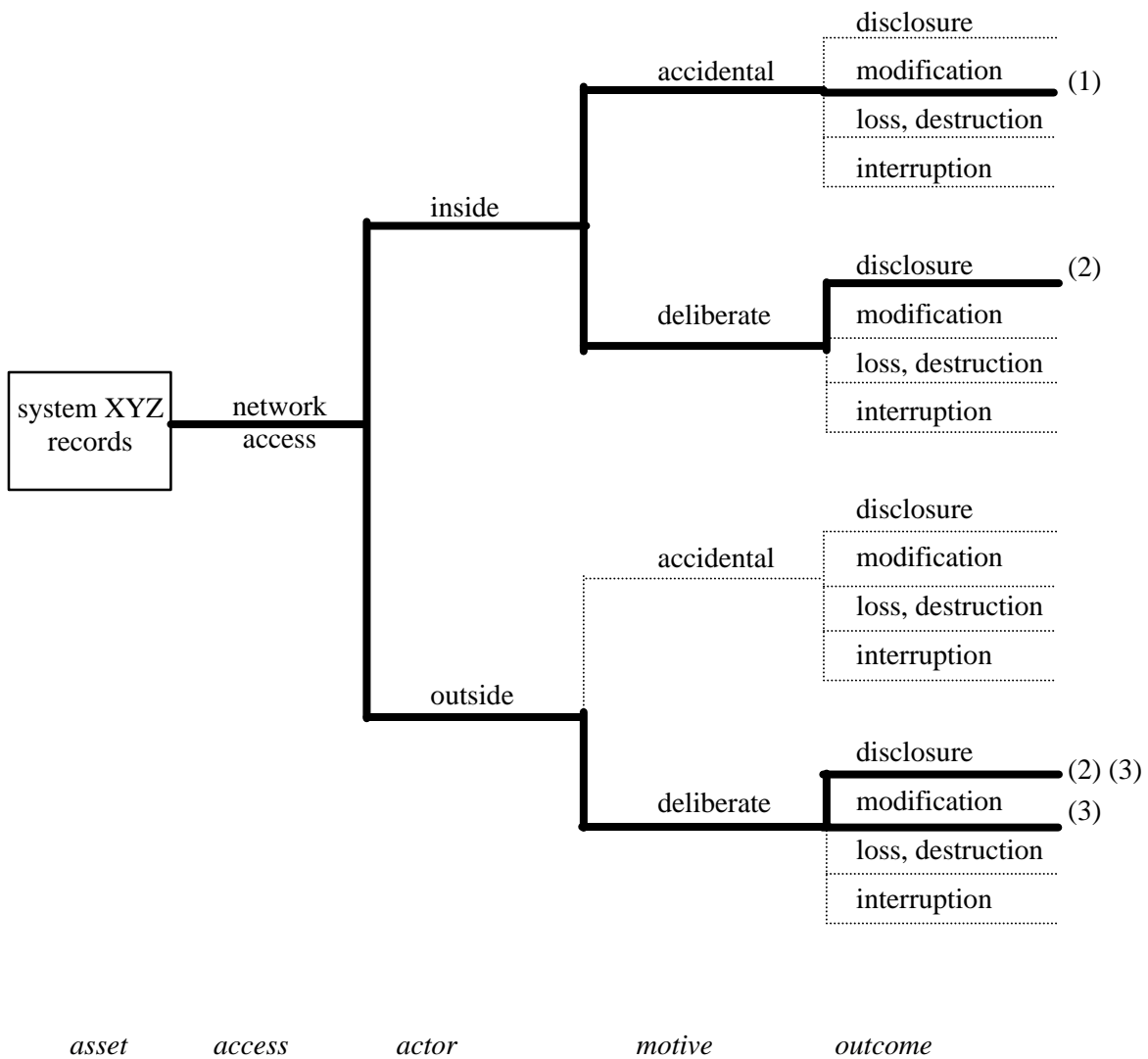


Figure 5. Areas of Concern Mapped to the Human Actors Using Network Access Threat Tree

The numbers at the end of the branches in Figure 5 correspond to the area of concern in Table 1. The dark lines represent threats to the critical assets, while the light, dashed lines indicate that no threat has been identified. The analysis team must map all areas of concern for a critical asset to the appropriate trees of the generic threat profile. Notice that only four threats were identified from the areas of concern.

Next, the analysis team must perform a gap analysis to determine if there are any other threats to the information on system XYZ. During this gap analysis, the analysis team decided that if an insider could deliberately disclose information from the records, they could also modify or destroy them, or even deny access to them. The team then identified other threats to the records on system XYZ. In fact, the analysis

team felt that all threats except accidental actions by outsiders were applicable to the records on system XYZ. The same process is used for the other categories of threats, yielding a threat profile for the critical asset.

Figure 6 shows the complete range of threats for the *Human Actors Using Network Access* category. The analysis team could record additional information for the threats represented by the tree. This would provide additional contextual information for the threats identified during the gap analysis.

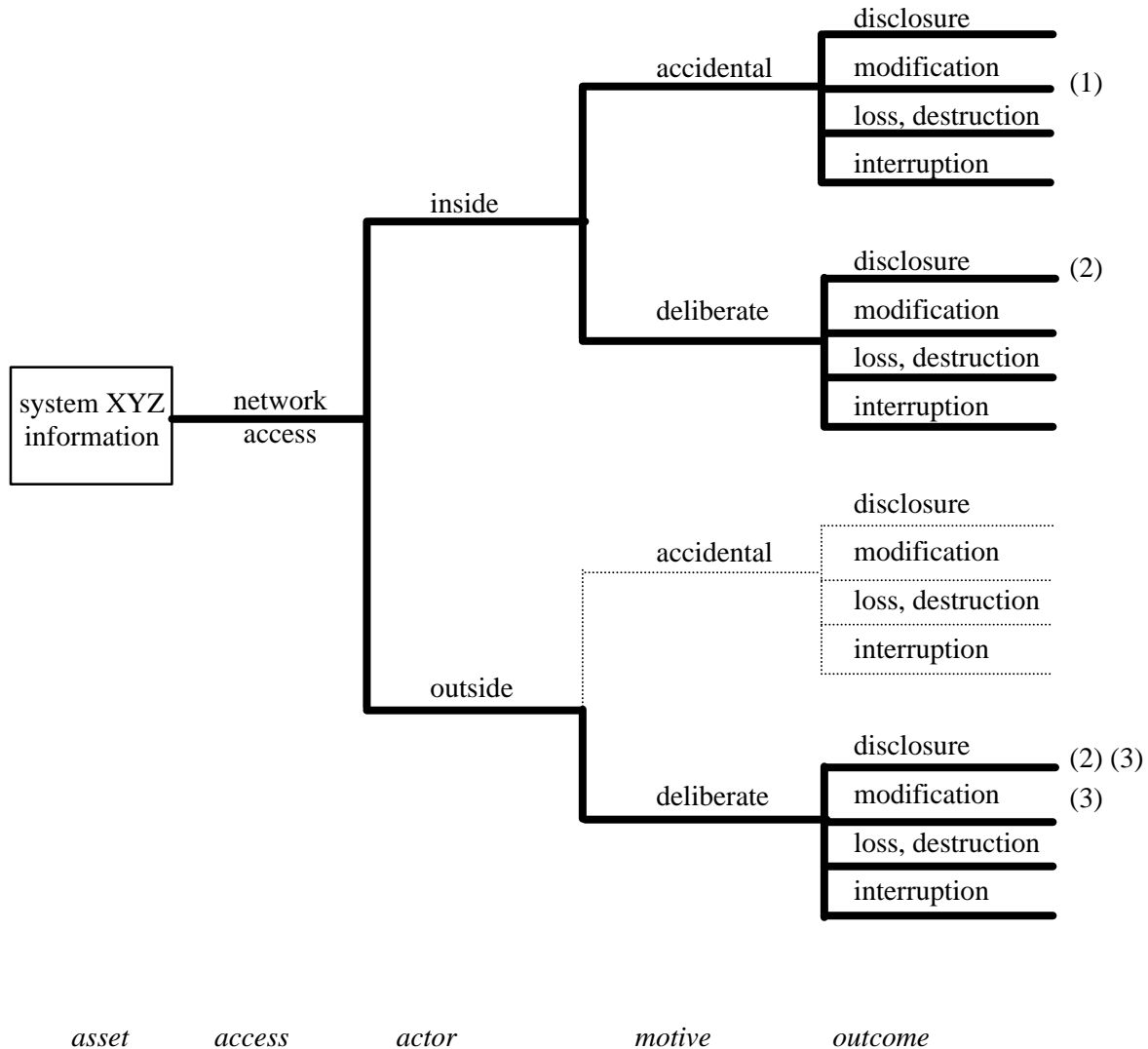


Figure 6. Example Threat Tree for Human Actors Using Network Access

3.3 Threat Profiles and Network Access Paths

Phase 2 of OCTAVE focuses on the information infrastructure. The analysis team examines the key operational components of the information technology infrastructure for weaknesses (technology vulnerabilities) that can lead to unauthorized action against the critical assets. In Phase 2, the analysis

team determines which components to evaluate, based on human threat actors exploiting vulnerabilities in the technology. In essence, the analysis team is looking at network access paths that can enable the threat scenarios identified for *Human Actors Using Network Access*. Figure 7 is the example threat tree for *Human Actors Using Network Access*, showing how key components and vulnerabilities relate to the threat tree. Note that the technology vulnerabilities create a means by which threat actors can exploit the vulnerabilities and access the critical asset.

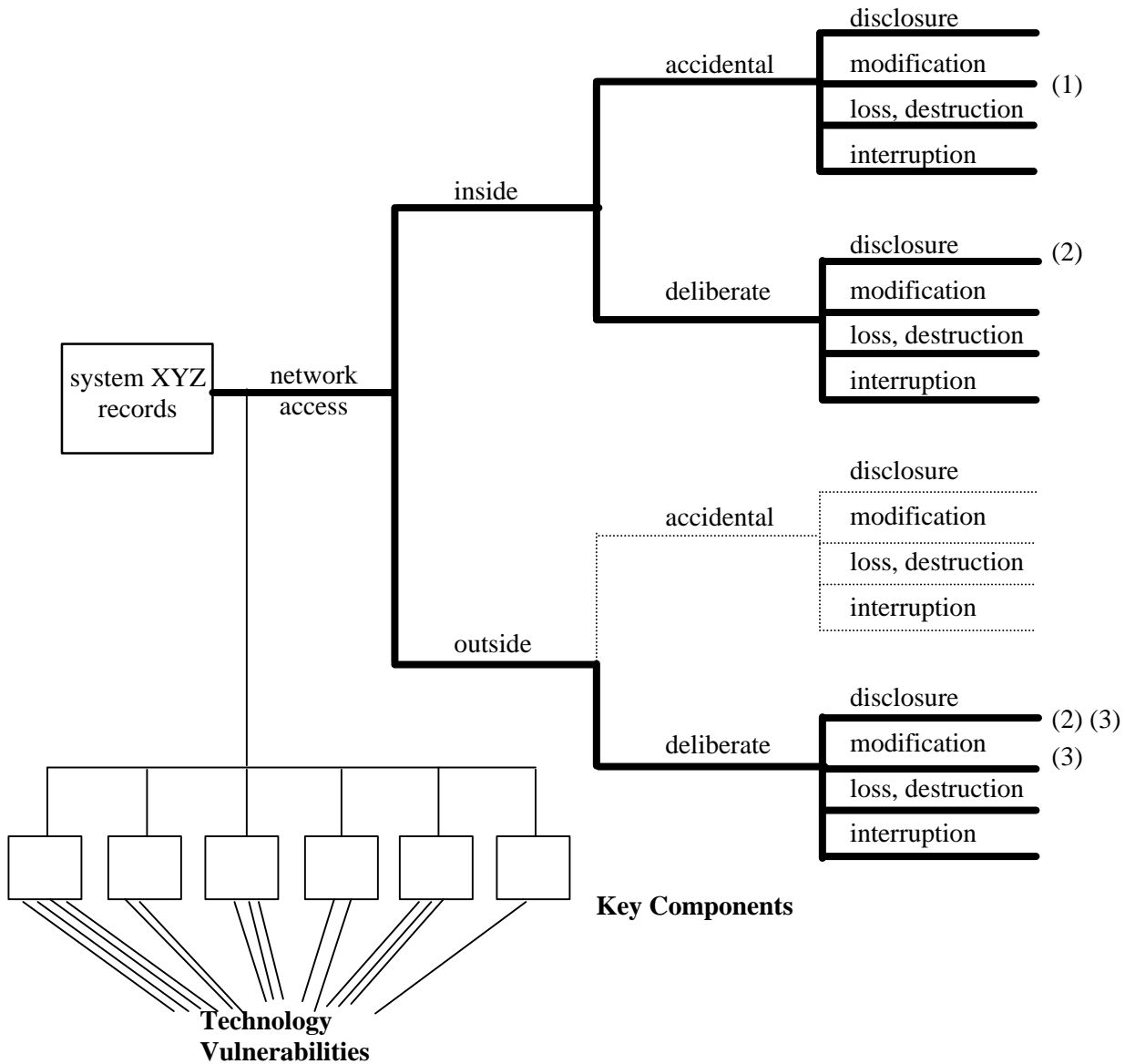


Figure 7. Technology Vulnerabilities and Network Access Paths

3.4 Creating and Analyzing Risk Profiles for Critical Assets

Once the assets, threats, and vulnerabilities have been identified in Phases 1 and 2, an organization is positioned to analyze the information and to identify the information security risks. During Phase 3, a risk profile is created for each critical asset. The risk profile for a critical asset consists of:

- the threat profile for that critical asset
- narrative descriptions of the resulting impact(s) to the organization
- qualitative values of those impacts to the organization

The risk impacts are based on the outcomes of the threats – disclosure, modification, loss or destruction, and interruption of access.

The goal is to reduce the risks to the critical asset through a combination of these actions:

- implementing new security practices within the organization
- taking the actions necessary to maintain the existing security practices
- fixing identified vulnerabilities

4.0 Summary

OCTAVE is a self-directed information security risk evaluation that enables organizations to make information-protection decisions based on risks to the confidentiality, integrity, and availability of their critical information technology assets. An interdisciplinary analysis team consisting of an organization's staff members manages the evaluation process and makes decisions about protecting the organization's critical assets.

To make the best possible information-protection decisions, it is essential to identify the threats to the critical assets. In OCTAVE, the range of potential threats is represented visually in tree structures. Collectively, the set of tree structures across all sources of threat is called the threat profile. The analysis team uses the threat profile to identify a range of threats to each critical asset. Once the analysis team understands the threats to the critical assets, it can then start to understand the risks to the organization and take steps to mitigate those risks.

5.0 References

1. Alberts, Christopher J.; Behrens, Sandra G.; Pethia, Richard D.; & Wilson, William R. *Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVESM) Framework, Version 1.0* (CMU/SEI-99-TR-017). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, June 1999.
2. National Security Telecommunications and Information Systems Security Committee. *Index of National Security Telecommunications Information Systems Security Issuances* (NSTISSI No. 4014). Ft. Mead, MD: NSTISSC Secretariat, January 1998.
3. Howard, John D. & Longstaff, Thomas A. *A Common Language for Computer Security Incidents* (SAND98-8667). Albuquerque, NM: Sandia National Laboratories, 1998.
4. Hutt, Authur E.; Bosworth, Seymour; & Hoyt, Douglas B. *Computer Security Handbook, 3rd ed.* New York, NY: John Wiley & Sons, Inc. 1995.
5. Parker, Donn B. *Fighting Computer Crime*. New York, NY: John Wiley & Sons, Inc. 1998.