9

Conducting the Risk Analysis (Process 7)

OCTAVE is focused on building an organizationwide view of information security risks. Up to this point in the evaluation you have collected data about three of the components of risk—threat, asset, and vulnerability. Your analysis activities have focused on critical assets, how they are threatened, and how they are technologically vulnerable. Now you broaden your view by considering the organization. You examine how threats to your organization's critical assets can affect its business objectives and its mission.

Process 7 begins phase 3 of the OCTAVE Method, Develop Security Strategy and Plans. This process creates the link between critical assets and what is important to your organization, putting your organization in a better position to manage the uncertainty that it faces.

9.1 Overview of Process 7

One of the evaluation attributes presented in Chapter 2 was the *focus on risk*. This attribute requires you to look beyond the immediate consequences (outcome) of the threat to a critical asset and place it in the context of what is important to your organization (impact). Up to this point in OCTAVE, you have collected data that will help you examine the security threats that affect your organization's mission and business objectives. In process 7 the focus shifts to risk identification and analysis.

Process 7 Workshop

The workshop for process 7 includes the core analysis team members as well as supplemental personnel, if needed. Your team, including supplemental members, should have the following skills:

- Understanding of the organization's business environment
- Understanding of the organization's information technology environment
- Good communication skills
- Good analytical skills

If you decide to supplement the skills of your analysis team, you should consider including people who understand the specific context of your business environment (e.g., people from the legal department, strategic planners, people from the business continuity office, policy managers). Your team needs these

skills, because process 7 requires you to examine how threats to critical assets affect the business objectives and mission of your organization.

An experienced analysis team can complete the activities in about 4½ to 6 hours. The activities of process 7 are summarized in Table 9-1.

TABLE 9-1 Process 7 Activities

Activity	Description
Identify the impact of threats to critical assets	The analysis team defines impact descriptions for threat outcomes (disclosure, modification, loss, destruction, interruption). The impact description is a narrative statement that describes how a threat ultimately affects the organization's mission.
Create risk evaluation criteria	The analysis team creates evaluation criteria that will be used to evaluate the risks to the organization. Evaluation criteria define what constitutes a high, medium, and low impact.
Evaluate the impact of threats to critical assets	The combination of a threat and the resulting impact to the organization defines the risk to the organization. The analysis team reviews each risk and assigns it an impact value (high, medium, or low).

Risk

Risk is the possibility of suffering harm or loss. It is the potential for realizing unwanted negative consequences of an event [Rowe 88]. It refers to a situation in which a person could do something undesirable or a natural occurrence could cause an undesirable outcome, resulting in a negative impact or consequence.

A risk comprises an event, uncertainty, and a consequence. In information security, the basic event in which we are interested is a threat. Uncertainty is embodied in much of the information you have gathered during the evaluation. The uncertainty concerns whether a threat will develop as well as whether your organization is sufficiently protected against the threat actor. In many risk methodologies, uncertainty is represented using likelihood of occurrence, or probability. As Section 9.3 explains, there is a lack of objective data for certain types of information security threats, making it difficult to use a forecasting approach based on probability. To handle the uncertainty inherent in risk, we propose an analysis technique based on scenario planning.

Finally, the consequence that ultimately matters in information security risk is the resulting impact on the organization due to a threat. Impact describes how the organization would be affected based on the following threat outcomes:

- Disclosure of a critical asset
- Modification of a critical asset
- Loss/destruction of a critical asset
- Interruption of a critical asset

The outcomes listed above are directly related to assets and describe the effect of the threat on an asset. However, the impact is focused on the organization; it is the direct link back to the organization's mission and business objectives. This chapter shows you how to explicitly identify the risks to your organization's critical assets. We begin looking at risk in the next section, as we present an approach for describing the organizational impact of threats to critical assets.

9.2 Identify the Impact of Threats to Critical Assets

Risk broadens the view of threat by considering how threats ultimately affect an organization. In this activity, you create and record narrative descriptions of potential impacts that can result from threats to your critical assets. As you do this, you establish the link among assets, threats, and what is important to your organization (i.e., your business objectives), providing you with a basis on which you can analyze your risk.

Step 1: Review Information

Before you work though the steps in this activity, you need to review information about your critical assets. This is important, because you are building on information from process 4, which you probably completed a while ago. Specifically, we suggest that you look at the following for each critical asset:

- Security requirements
- Threat profiles
- Areas of concern

These data indicate what is important about each critical asset (security requirements) and how they are threatened (threat profile and areas of concern). You need to make sure that this information is fresh in your mind as you move on to step 2.

Step 2: Create Narrative Impact Descriptions

Your objective in this step is to record a narrative description of the potential impact on your organization of threats to your critical assets. Note the difference in the use of the terms "outcome" and "impact." An outcome is the immediate result of a threat; it centers on what happens to an *asset*. There are four possible threat outcomes: disclosure, modification, loss/destruction, and interruption. The impact, on the other hand, is broader, describing the effect of a threat on an organization's *mission and business objectives*. Consider the following example.

> *Someone inside the organization uses network access to deliberately modify the medical records database. This could result in patient death, improper treatment delivered to patients, lawsuits, and additional staff time to correct the records.*

In this example the threat outcome is modification. Notice that modification is tied to an asset, namely, the medical records database. Now consider how modification of the medical records database can affect the organization. The potential impact on the organization includes the following: patient death, improper treatment delivered to patients, lawsuits, and additional staff time to correct the records. Again, an outcome is the immediate result of the threat actor and centers on assets, whereas the impact considers the resulting effect on the operations and people in the organization.

We ask you to consider impact in the following areas during this activity:

- Reputation/customer confidence
- Safety/health issues
- Fines/legal penalties
- Financial
- Productivity

These impact areas are contextual and should be tailored to meet the needs of your organization. Before you conduct an evaluation, you should determine which areas of impact to consider. One way to determine unique areas for your organization is to consider its business objectives and make sure that impact areas are linked to your key business objectives. For example, a military organization may add combat readiness as an area of impact.

To conduct step 2, select one of your critical assets. Review the threat profile for that critical asset. Make sure that you note which of the threat outcomes (disclosure, modification, loss/destruction, interruption) are part of the scenarios in the profile. Next, answer the following questions for each outcome that appears in at least one of the scenarios:

- What is the potential impact on the organization's reputation?
- What is the potential impact on customer confidence?
- What is the potential impact on customers' health or safety?
- What is the potential impact on staff members' health or safety?
- What fines or legal penalties could be imposed on the organization?
- What is the potential financial impact on the organization?
- What is the potential impact on the organization's or customers' productivity?
- What other types of impact could occur?

Continue with this activity until you have described the impact in relation to all critical assets. Make sure that you document your results.

Let's looks at our example to see how MedSite's analysis team completed this activity, specifically, how they created impact descriptions for PIDS. The team members reviewed the information that they had recorded for PIDS. They reviewed the threat profile, the security requirements, and areas of concern. (See Appendix A for a summary of this information for PIDS.)

The team members noted that at least one threat resulted in disclosure of PIDS information. Likewise, at least one threat resulted in modification, loss/destruction, and interruption of access to PIDS information. Thus, all threat outcomes were possible. As a result, the team would have to consider impacts in relation to all four outcomes. They discussed the key questions for each outcome and documented the resulting types of impact on MedSite. These are shown in Figure 9-1.

We have just shown you how to begin expanding threats into risks by considering the impact on the organization. Next, we present an approach for setting qualitative risk levels for your organization.

Outcome	Impact Description
Disclosure	• Failure to safeguard privacy would result in loss of credibility of medical treatment facility/organization.
Modification	• Incorrect modifications could affect appointments and productivity. • Work could be affected if modifications were made and we were unable to determine the extent easily. Verification of patient information would be tedious. • Patients' lives and health could be affected due to improper changes to treatment plans or medical records. • Medical treatment facility could lose credibility, causing patients to seek care from another source.
Loss/destruction	• The information in PIDS would be nearly impossible to reconstruct in a timely manner. Just trying to verify and reenter what was lost between the last backup and the present would take all our time and resources.
Interruption	• An interruption could have a direct impact on our role in this community. We are rendered virtually helpless without PIDS capability. We have become computer-dependent in order to function. • Our organization cannot deliver effective or efficient health care without PIDS.

FIGURE 9-1 Impact Descriptions for PIDS

9.3 Create Risk Evaluation Criteria

During this activity you define your organization's tolerance for risk by creating evaluation criteria. These criteria are measures against which you evaluate the types of impact you described during the previous activity. An organization must explicitly prioritize known risks, because it cannot mitigate all of them. Funding,

staff, and schedule constraints limit how many and to what extent risks can be addressed. This activity provides decision makers with additional information that they can use when establishing mitigation priorities.

Step 1: Review Information

You need to review relevant background information to help you define evaluation criteria. Such information includes the following:

- Strategic and/or operational plans that outline the major business objectives of your organization
- Legal requirements, regulations, and standards of due care with which your organization must comply
- Insurance information related to information security and information protection
- Results from other risk management processes used by your organization

You can also use the narrative impact information that you documented during the previous activity. Your goal is to develop an understanding of any existing organizational risk limits based on strategic and operational plans, liability, and insurance-related issues. These data are important in shaping evaluation criteria.

Evaluation criteria are highly contextual. For example, while $1 million may represent a high impact for one organization, it might signify only a medium or low impact for another. Also, some organizations will have risks that could result in a loss of life, but others will not. The contextual nature of evaluation criteria is the reason every organization must define its own criteria and why you need to review relevant background information.

Step 2: Define Evaluation Criteria

In this step you define your organization's evaluation criteria. Discuss the following questions for each area of impact (see previous activity for a discussion of areas of impact):

- What defines a "high" impact on the organization?
- What defines a "medium" impact on the organization?
- What defines a "low" impact on the organization?

You are trying to define specific measures that constitute high, medium, and low risks for your organization in each case. For example, a low impact on productivity might be three lost days, whereas a high impact might be three weeks. As always, make sure that you record this information.

Now let's look at evaluation criteria in the context of an example. The analysis team at MedSite included a member from the risk management department to help them construct evaluation criteria. Prior to the process 7 workshop, the staff member from the risk management department worked with one of the analysis team members to collect background information. They gathered the organization's operational plan and information about legal requirements and regulations.

Prior to the workshop, all members of the team reviewed the information. They selected the following areas of impact for which to create evaluation criteria:

- Reputation/customer confidence
- Life/health of customers
- Productivity
- Fines/legal penalties
- Finances
- Facilities

The team discussed what constitutes a high, medium, and low impact on the organization for each of the relevant areas and recorded the information. Figure 9-2 highlights the evaluation criteria for reputation/customer confidence. You will find a complete set of criteria for the example in Appendix A of this book.

Scenario Planning and Probability

You might have noticed that we are focusing only on impact at this point. A second commonly used risk measure is probability. For information security risks, probability is a more complex and imprecise variable than is normally found in other risk management domains, because risk factors are constantly changing. Probability is highly subjective in the absence of objective data and must be used carefully during risk analysis.

Because objective data for certain types of information security threats (i.e., human actors exploiting known vulnerabilities) are lacking, it is difficult to use a forecasting approach based on probability. Without objective data, it is impossible to develop a reliable forecast of the future [HBR 99]. What you can

Evaluation Criteria

Area of Impact	High	Medium	Low
Reputation/ customer confidence	• Reputation irrevocably destroyed or damaged • Loss of rating or accreditation by review organizations • More than 30 percent drop in customers due to loss of confidence	• Reputation damaged; some effort and expense required to recover • Reduction or warning of reduction of rating or accreditation by authorizing organizations • 10 to 30 percent drop in customers due to loss of confidence • Public violations of Privacy Act: disclosure to (1) personnel within the medical treatment facility without the need to know; (2) anyone who violates the Privacy Act and reveals sensitive medical information • Patient driven to seek care from another source	• Reputation minimally affected; little or no effort or expense required to recover • No change in rating or accreditation by authorizing organizations • Less than 10 percent drop in customers due to loss of confidence • Nonpublic violation of Privacy Act (disclosure to personnel within the medical treatment facility with a need to know—trusted agent)

FIGURE 9-2 Evaluation Criteria

do, however, is carefully analyze threats to limit the range of potential options, so that you become able to manage your risk. In information security, you can define a range of threats that could affect a critical asset, but you cannot reliably predict which scenario(s) will occur. However, by broadly defining the range of threats that your organization faces, you can make fairly certain that those that develop do so within the defined bounds.

The analysis approach that we are describing here is derived from a technique called scenario planning. A range of threat scenarios, or a threat profile, is

constructed for each critical asset. The scenarios in each threat profile represent those in the probable range of outcomes, not necessarily the entire range. Because data with respect to threat probability are limited for the scenarios, they are assumed to be equally likely [Van der Heijden 97]. Thus, priorities are based on the qualitative impact values assigned to the scenarios.

Probability values can be factored into prioritization, but you must take care when doing so. Remember, probability is a forecasting technique based on the premise that you can forecast threat probability with reliable precision. Thus, in many cases you may be forcing decisions based on probability forecasts that are nothing more than guesswork. Nonetheless, incorporating probability into a risk analysis continues to be a popular topic. Section 9.5 considers an approach for incorporating subjective probability in OCTAVE.

When Should You Create Evaluation Criteria?

Note the following two conditions governing risk evaluation criteria:

- There is one set of evaluation criteria for all assets; the criteria are not unique to an asset.
- Evaluation criteria are created for predefined areas of impact, which are related to the organization's key business objectives.

Because evaluation criteria are asset-independent and address broad organizational issues, you could create them earlier in the evaluation process. Some organizations decide to add this activity to process 1, the senior management workshop. By doing so, these organizations are able to gather input from senior managers with a broad perspective on organizational issues. Another idea is to create evaluation criteria when preparing to conduct the OCTAVE Method, as part of your tailoring activities.

If you have previously conducted the OCTAVE Method in your organization, you could use the set of criteria that you already created. If you decide to use evaluation criteria from a previous evaluation, remember to review them and adjust them as appropriate before using them in the current evaluation.

No matter when you create evaluation criteria, it can be a long process. You will probably find that it is also an iterative process. An organization will often revisit its evaluation criteria and adjust them after trying to use them. However, once you are satisfied with your criteria, you have a useful tool for interpreting risk. In the next activity we show how you use this tool.

9.4 Evaluate the Impact of Threats to Critical Assets

This activity builds upon the first two. You use the evaluation criteria that you created previously to evaluate the impact descriptions that you developed earlier during the first activity of process 7. By doing this, you are able to estimate the impact on the organization for each threat to a critical asset. The ultimate result is that you can now establish priorities to guide your risk mitigation activities during process 8.

Step 1: Review Information

Before you evaluate your risks, you need to review the information gathered so far from earlier processes. Specifically, we suggest that you look at the evaluation criteria and the following for each critical asset:

- Threat profiles
- Impact descriptions

These data provide you with scenarios that threaten your critical assets (threat profiles), the resulting impact (impact descriptions), and risk measures for your organization (evaluation criteria). Together, they provide you with a picture of the information security risks that your organization is facing.

Step 2: Evaluate Risk Impact

For each critical asset, first review the impact descriptions for each threat outcome (disclosure, modification, destruction/loss, interruption). Some outcomes will have more than one impact description associated with them. Next evaluate each impact description by assigning it an impact measure (high, medium, or low). Using the qualitative evaluation criteria that you created during the previous activity as a guide, continue evaluating impacts until you have evaluated all of the impacts for each critical asset. Make sure you record your results.

Finally, when you add impact values to the threat profile, you create a risk profile. Essentially, you have created a set of risk scenarios for a critical asset.

Let's see how the team at MedSite evaluated impacts. The analysis team and the representative from MedSite's risk management department started with

PIDS. They reviewed its threat profiles and impact descriptions, as well as the evaluation criteria, and evaluated each impact that they recorded for PIDS.

Let's specifically look at how the team evaluated the impact of modification of PIDS information. In reviewing the PIDS threat profile, they found the following threats with an outcome of modification in the profile:

- People inside MedSite can use network access to modify PIDS information accidentally.
- People inside MedSite can use network access to modify PIDS information deliberately.
- Outsiders (i.e., attackers) can use network access to modify PIDS information deliberately.
- People inside MedSite can use physical access to modify PIDS information deliberately.
- People outside MedSite can use physical access to modify PIDS information deliberately.
- A virus can modify PIDS information.

Note that the above threats are textual versions of PIDS threat profile branches. Next, the team reviewed the various types of impact. Consider the following impact from Figure 9-1:

> *Medical treatment facility could lose credibility, causing patients to seek care from another source.*

This impact is related to the area of reputation/customer confidence, for which the evaluation criteria are shown in Figure 9-1. After the team discussed this impact and examined it in relation to these criteria, they felt that MedSite's reputation would be damaged, but that it could be recovered with some effort and expense. Thus, the team assigned the value of "medium" to this impact. Figure 9-3 shows the impact values for the levels of impact resulting from modification of PIDS information.

Notice that there are four levels of impact associated with modification of PIDS information. Each impact was evaluated, and its value recorded in the right column. Three were assigned a value of medium, while the fourth was judged to be high. The team evaluated all levels of impact for PIDS and the other critical assets. You will find the complete set of evaluation results in Appendix A.

Outcome	Impact Description	Impact Measure
Modification	• Incorrect modifications could affect appointments and productivity.	Medium
	• Work could be affected if modifications were made and we were unable to determine the extent easily. Verification of patient information would be tedious.	Medium
	• Patients' lives and health could be affected due to improper changes to treatment plans or medical records.	High
	• Medical treatment facility could lose credibility, causing patients to seek care from another source. We can recover our reputation.	Medium

FIGURE 9-3 Impact Values for Modification of PIDS Information

The final step is to create what we call a risk profile. To do this, you simply append the impact values to the trees in the threat profile and record the range on the risk profile—in this case, high to medium. Figure 9-4 shows the threat tree for human actors using network access for PIDS with all impact values added. Note that a solid line in Figure 9-4 indicates the existence of a risk, while a dashed line indicates no risk to the asset.

If you have difficulty using the evaluation criteria as you evaluate the impact descriptions, then one of the following might be occurring:

- The impact *description* might be too vague to enable you to match it to the evaluation criteria. If this is the case, you need to refine the impact descriptions by making them more specific.
- The evaluation *criteria* might not be specific enough to enable you to assign measures to impact descriptions. In this case you need to refine the evaluation criteria by making them more specific.

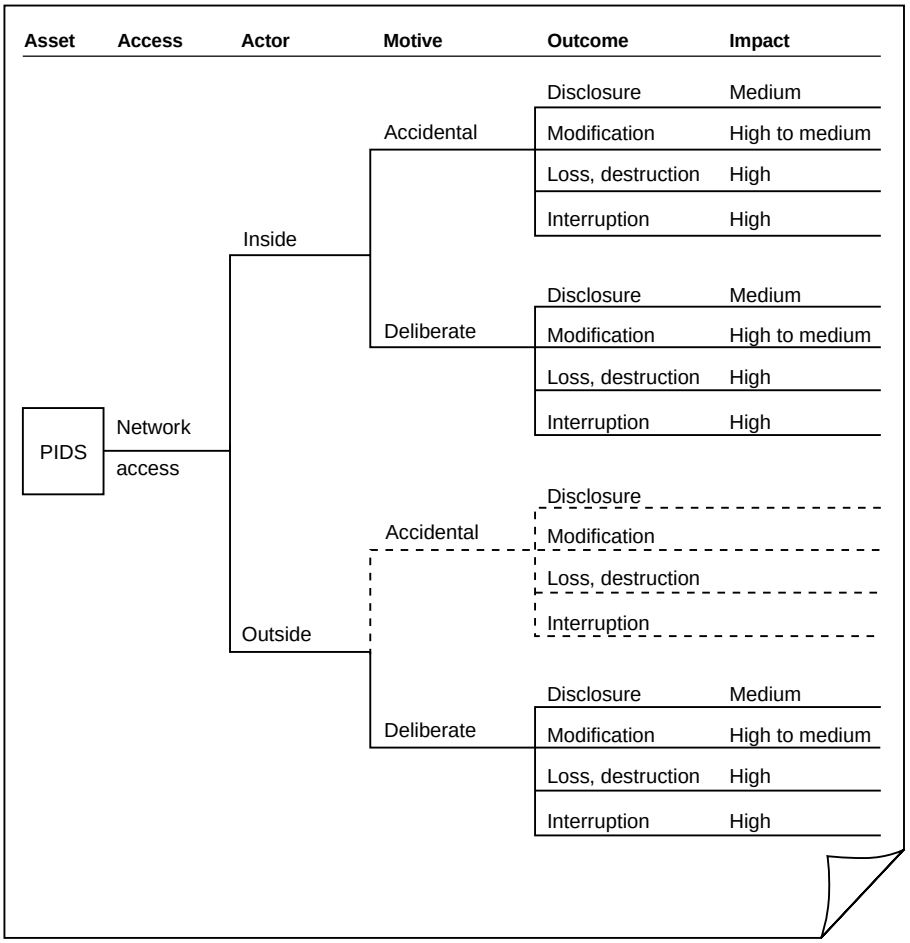

FIGURE 9-4 Part of PIDS Risk Profile: Human Actors Using Network Access Tree

In the second case you might also want to check any impact values that were assigned using the first set of criteria to make sure that they are consistent with the refined criteria.

This completes the basic risk analysis activities for OCTAVE. The next section presents a special topic: incorporating probability into the risk analysis.

9.5 Incorporating Probability into the Risk Analysis

So far this chapter has focused on an analysis technique based on scenario planning. We incorporated this technique in OCTAVE, because the lack of objective data for certain types of information security threats makes it difficult to incorporate a forecasting approach based on probability. However, we have found that there is considerable interest in using probability during a more traditional risk analysis. This section presents some basic concepts of probability and shows how you can include probability in the activities of process 7.

9.5.1 What Is Probability?

We define probability as the likelihood that an event will occur. We first consider the *classical concept* of probability. This concept is the oldest historically and was originally developed in connection with games of chance [Bernstein 96]. For example, consider a die, which is simply a cube with six faces. Because of its symmetry, each face is as likely to come up as any other. Thus, you could easily determine the probability of one face coming up with a roll of the die as 1 in 6. The key for this concept of probability is that all possibilities must be equally likely to occur.

Frequency

Next, we consider the *frequency interpretation* of probability. This interpretation indicates that the probability of an event occurring (or a given outcome occurring) is the proportion of the time that similar events will occur over a long period of time. Note that when using the frequency interpretation of probability, you cannot guarantee what will happen on any particular occasion. Thus, you actually never really "know" the probability that an event will occur, because you will not be able to collect enough information to know precisely what will happen in the long run. Although you cannot know the exact value of a probability, you can estimate it by observing how often similar events have occurred in the past. Estimates of probability made after observing similar events are useful because of the *law of large numbers* [Freund 93]. This law states that as the number of times a situation is repeated becomes larger, the proportion of successes tends toward the actual probability of success. For example, consider multiple flips of a coin. If you flip a coin repeatedly and chart the accumulated proportion

of time that you get heads, you will find that over time the proportion comes closer and closer to 1 in 2 (the probability of getting heads with each flip).

A common example that uses the frequency interpretation of probability is weather forecasting. If the forecast calls for a 60 percent chance of rain, it means that under the same weather conditions, it will rain in 60 percent of cases. Next, let's consider a variation of this case—how do you estimate the probability of something that occurs just once? Consider how doctors estimate the probability of how long it will take a patient to recover from an illness. A doctor can check medical records and discover that in the past, 50 percent of the patients recovered within two months under a specific treatment plan. By using this information from similar cases, the doctor can predict that there is a 50 percent probability that the patient will recover within two months.

You can probably see how complicated this can get. It is not always easy or straightforward to determine which cases are similar to the one that you are considering. In the case of the patient, the doctor might consider not just the treatment plan being prescribed but also the patient's age, gender, height, and weight, among other factors. This approach can be difficult and requires individual judgment, indicating how easy it is for two individuals to arrive at different probabilities for the same event.

Subjective Probability

The final type of probability that we will discuss is *subjective* probability. This approach is often used in situations where there is very little direct evidence. You might have only some indirect, or collateral, information, educated guesses, intuition, or other subjective factors to consider [Freund 93]. A person determines a probability based on what he or she *believes* to be the likelihood of occurrence. The key word here is "believes." Different people assess probabilities differently, based on their personal evaluation of a situation. One disadvantage of this approach is that it is often hard for people to estimate probability, and the same person can end up estimating different probabilities for the same event using different estimating techniques.

Probability and Information Security

In information security, you are interested in estimating the likelihood that a threat will actually materialize. For some types of security threats, you have information upon which you can draw. For example, you can use the frequency

data to estimate the probability of natural disasters (e.g., floods, earthquakes) in your region. You might also be able to use the frequency of occurrence to estimate the probability of some systems problems, such as system crashes and susceptibility to viruses. However, for some other types of threats there are no frequency data.

How would you estimate the probability of an attacker viewing confidential customer data from your organization's customer database? How much company data do you have to estimate the probability of this attack? Most likely, your organization has not collected sufficient data about such attacks to enable an estimation of probability based on frequency of occurrence. If it has occurred, it has probably happened only once or twice. In addition, you cannot be sure how many times this attack has occurred but gone undetected. What about industry data? Is this the kind of information that companies readily disclose? Many attacks of this type go unreported, making it difficult to obtain sufficient data to derive probability based on frequency models. Finally, even if you had some industry data about these types of attacks, how do you establish which events are similar? For example, does information about past attacks in the banking sector apply to organizations in the manufacturing sector? All of these factors make a frequency-based estimation of probability difficult and time-consuming, if not impossible. That leaves us with subjective probability for threats resulting from human attackers.

Subjectively estimating probability for attacks by human threat actors is tricky. You need to consider the following factors:

- Motive—how motivated is the attacker? Is the attacker motivated by political concerns? Is the attacker a disgruntled employee? Is an asset an especially attractive target for attackers?
- Means—which attacks can affect your critical assets? How sophisticated are the attacks? Do likely attackers have the skills to execute the attacks?
- Opportunity—how vulnerable is your computing infrastructure? How vulnerable are specific critical assets? (Note that this question is linked to the vulnerability data that you gathered in process 6.)

When estimating the above factors, people typically rely upon their experience to make educated guesses about the likelihood of attacks occurring. You would need experience with networked systems security as well as an understanding of the industry sector in which an organization operates. Note that some

people do not have sufficient experience to estimate probability using subjective techniques. In fact, probabilities estimated by inexperienced people can actually skew the results of a risk analysis.

In general, you must be careful when incorporating probability into your risk analysis. The next section explains how you can incorporate probability into the activities of process 7 using a combination of frequency data and subjective estimation.

9.5.2 Probability in the OCTAVE Method

We propose using a combination of frequency and subjective probability into the OCTAVE Method's risk analysis activities. There are three activities to add if you choose to do this:

1. Describe the probability of threats to critical assets.
2. Create probability evaluation criteria.
3. Evaluate the probability of threats to critical assets.

Step 1: Describe the Probability of Threats to Critical Assets

In addition to identifying the impacts of threats, you identify probability. You gather information related to the factors that contribute to determining probability. Consider the following questions for each threat profile:

- Which critical assets are likely targets of human threat actors?
- What are the motive, means, and opportunity of each human threat actor who might use network access to violate the security requirements of the critical asset?
- What are the motive, means, and opportunity of each human threat actor who might use physical access to violate the security requirements of the critical asset?
- What historical data for your company or domain are available for all threats in the threat profile? How often have threats of each type occurred in the past?
- What unusual current conditions or circumstances might affect the probability of the threats in the threat profile?

By answering the above questions, you gather both subjective and objective data about threats to your critical assets. You can then use them to estimate threat probability. Notice that the first three questions and the last question are subjective in nature, while the fourth question relates to any objective threat data you may have. You need to make sure that you record all subjective information and objective data for each type of threat to your critical assets.

Step 2: Create Probability Evaluation Criteria

In addition to developing evaluation criteria for impact, you also create evaluation criteria for probability. These criteria are measures against which you will evaluate each threat to establish a qualitative probability value for that threat. Evaluation criteria for probability indicate how often threats occur over a common period of time. When you create evaluation criteria for probability, you define measures for high, medium, and low likelihood of occurrence for your organization.

Review the probability information that that you gathered during the previous activity and answer the following questions:

- What defines a “high” likelihood of occurrence?
- What defines a “medium” likelihood of occurrence?
- What defines a “low” likelihood of occurrence?

Remember, your goal is to define probability measures using any objective data that you have in addition to your subjective experience and expertise. You also need to make sure that your criteria are meaningful to your organization. As always, record your results.

Let’s examine what evaluation criteria might look like for our sample organization. At MedSite the analysis team supplemented their skills by including the following:

- A member of ABC Systems who had extensive information technology security experience. This individual understands the range of possible attacks in the medical domain and the degree of skill required to execute each attack.
- A member from MedSite’s risk management department. This individual has background knowledge about many of the threat actors in the threat profile.

The expanded team reviewed background information. The people with information technology and risk management expertise provided valuable insight into creating frequency ranges for each probability level. Figure 9-5 shows the resulting probability evaluation criteria.

Notice that the criteria in Figure 9-5 use frequency of occurrence to define probability levels. Team members used the data that they had for certain sources of threat in conjunction with their subjective experience for those sources for which they had little or no objective data. Thus, despite the use of frequency in the criteria, this represents a highly subjective look at probability, and it should be noted as such.

Step 3: Evaluate the Probability of Threats to Critical Assets

Finally, in addition to evaluating the impact of each threat, you evaluate its probability. Review all relevant background information before you complete this activity. Make sure that you review threat profiles for each critical asset and the evaluation criteria for probability.

Select a critical asset. Assign each threat a qualitative probability value (high, medium, or low) based on (1) the probability information that you have gathered, (2) the probability evaluation criteria that you created, and (3) your team's collective experience and expertise.

If you find that your probabilities don't make intuitive sense—for example, if all of your threats are evaluated as "high probability"—you might want to go

Value	Frequency of Occurrence (subjective)
High	>12 times per year
Medium	1 time every year–11 times per year
Low	<1 time every year

FIGURE 9-5 MedSite's Probability Evaluation Criteria

back and adjust your probability criteria. Once you are satisfied with your evaluation results, the final step is to add probabilities to the risk profile.

At MedSite the expanded team (the analysis team plus supplemental personnel) assigned probability values to each threat in all threat profiles. Figure 9-6 shows part of the PIDS risk profile with probability added to the tree.

This concludes process 7. Chapter 10, which examines risk mitigation, revisits the topic of probability and looks at building risk mitigation plans for each critical asset and forming a protection strategy for organizational improvement.

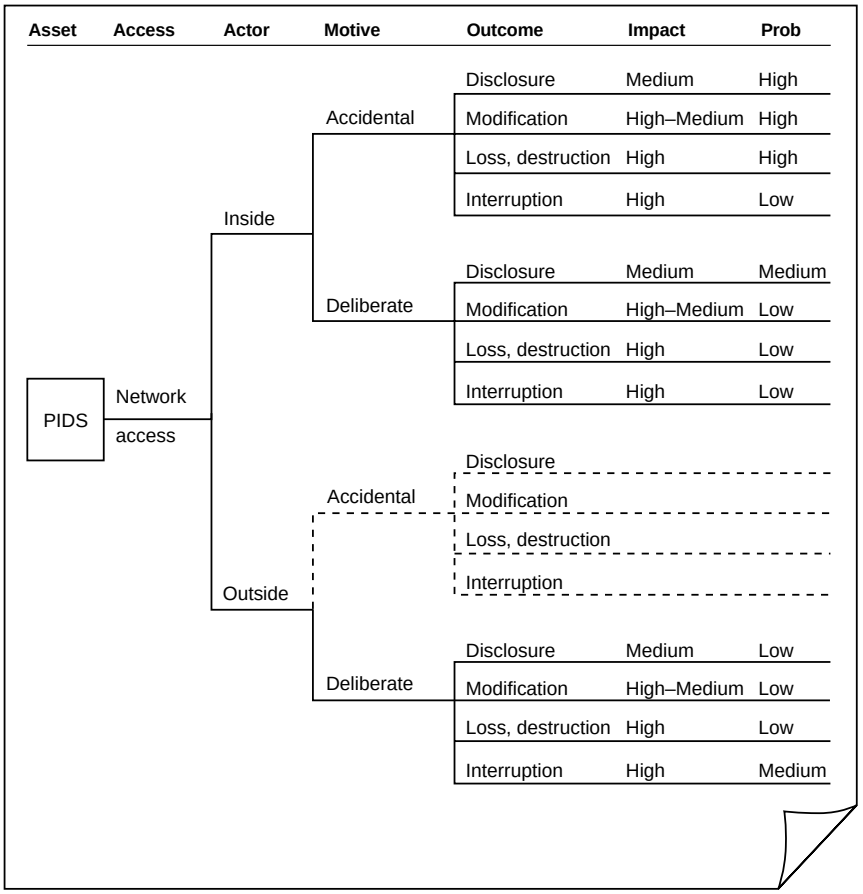

FIGURE 9-6 Part of the PIDS Risk Profile (Including Probability): Human Actors Using Network Access Tree