National Infrastructure Protection Center

Risk Management: An Essential Guide to Protecting Critical Assets

November 2002

Summary

As organizations increase security measures and attempt to identify vulnerabilities in critical assets, many are looking for a mechanism to ensure an efficient investment of resources to counter physical and cyber threats. One method is a risk management model that not only assesses assets, threats, and vulnerabilities but also incorporates a continuous assessment feature. This allows organizations to tailor their management of risk to the current situation as well as assess future risks. The management of risk impacts the bottom line of every organization, either in monetary terms or in terms of operational readiness and capability. Security managers and decision-makers that operate in any sector of the national infrastructure must have a sound methodology to manage both physical and cyber risks to their organization.

Introduction

The terrorist attacks of September 11, 2001 made security an urgent issue in both the public and private sectors. Any organization that plays a role in the nation's critical infrastructure is seeing a new level of threat. For example, one security issue that has received heightened attention is the cyber threat, as many analysts indicate that future attacks could involve an attack on computer networks. Many modern security programs, including those for national computer networks, are adopting a risk management approach as a means to counter this growing threat within the context of dwindling resources.

Risk avoidance, the model used by professionals to address security in the past, focused only on *preventing* loss or damage without reference to the degree of risk. Risk management, in contrast:

- Identifies weaknesses in an organization or system (such as a water system, electric power grid, or building);
- Offers a rational and defendable method for making decisions about the expenditure of scarce resources and the selection of cost-effective countermeasures to protect valuable assets;
- Improves the success rate of an organization's security efforts by emphasizing the communication of risks and recommendations to the final decision-making authority;
- Helps security professionals and key decision-makers answer the question: "How much security is enough?"

This document will help managers considering security reviews or risk assessments by providing guidance on how to review those assessments for thoroughness. Essentially, the Risk Management model is a threat appropriate response. The following sections define the terms used in the risk management cycle and describe the basic steps of such a cycle. Whether an organization plans to conduct risk management itself or hire a company to do it, the assessment should follow the steps in this guide.

> ***"A risk management approach can be applied at all levels of activity in our country – from federal agencies to state and local governments and across the public and private sector."***
>
> Raymond J. Decker
> Director, Defense Capabilities and Management
> Testimony before the Senate Committee on
> Governmental Affairs, October, 31 2001
> (GAO-02-208T)

Definitions[1]

Simply stated, *risk management* is a systematic and analytical process by which an organization identifies, reduces, and controls its potential risks and losses. This process allows organizations to determine the magnitude and effect of the potential loss, the likelihood of such a loss actually happening, and countermeasures that could lower the probability or magnitude of loss. Whereas a single countermeasure may seem intuitive to an analyst or security manager, alternative countermeasures should be identified and evaluated to select those which offer an optimal trade-off between risk reduction and cost. Organizations seek an "acceptable" level of risk that reflects the best *combination* of security and cost.

Risk is a function of assets, threats, and vulnerabilities. These terms are commonly used in a variety of ways in analysis. Therefore, it is useful to define how these terms are used and how they relate to each other in a risk management context. *Risk* is the

[1] These definitions were derived from material used by the Information Solutions Division of Veridian in presenting its course on Continuous Risk Management.

potential for some unwanted event to occur. Examples of unwanted events include the loss of information, money, organizational reputation or someone gaining unauthorized privileged access to your system. Risk is a function of the likelihood of the unwanted event occurring and its consequences; therefore, the higher the probability and the greater the consequences, the greater the risk. The likelihood of the unwanted event occurring depends upon threat and vulnerability.

Threat is the capability and intention of an adversary to undertake actions that are detrimental to an organization's interests. Threat is a function of the adversary only; it cannot typically be controlled by the owner or user of the asset. However, the adversary's intention to exploit his capability may be encouraged by a vulnerability in an asset or discouraged by an owner's countermeasures.

Vulnerability is any weakness in an asset or countermeasure that can be exploited by an adversary or competitor to cause damage to an organization's interests. The level of vulnerability, and hence level of risk, can be reduced by implementing appropriate security countermeasures.

An *asset* is anything of value (people, information, hardware, software, facilities, reputation, activities, and operations). Assets are what an organization needs to get the job done—to carry out the mission. The more critical the asset is to an organization accomplishing its mission, the greater the effect of its damage or destruction. An example is the loss of an organization's file and print server. This loss would significantly reduce an organization's ability to access and move data. The loss would have greater consequences if it occurred during a key operation or the server could not be repaired or replaced for several days. *Countermeasures* are actions or devices that mitigate risk by affecting an asset, threat, or vulnerability.

A Five Step Risk Assessment Model

Prior to beginning the analysis some time should be spent in preparation. The analyst should interview or brief the requestor (asset owner) to identify any constraints on the study and determine the goals and focus of the effort. The asset owner will best know what and where his or her assets are and their criticality to the organization. The analyst should also identify the *stakeholders* and determine their goals. Stakeholders are people or organizations that have a vested interest in the protection of an asset. For example, although an organization's Chief Information Officer may "own" his or her company's network, division or department heads have an interest in the availability and integrity of that network. With that knowledge, an analyst can begin the five steps of the Risk Management Model[2]:

1. Asset Assessment
2. Threat Assessment
3. Vulnerability Assessment

[2] E. Jopeck, The Risk Assessment: Five Steps to Better Risk Management Decisions, *Security Awareness Bulletin,* No. 3-97: 5–15.

4. Risk Assessment
5. Identification of Countermeasure Options.

Asset Assessment

In the Asset Assessment step, the security specialist (with the assistance of the asset owner) identifies and focuses only on those assets important to the mission or operation. By identifying and prioritizing these assets, an organization takes the first step towards focusing their resources on that which is most important. Most assets are tangible (e.g., people, facilities, equipment) others are not (e.g., information, processes, reputation). In infrastructure operations, information and automated processes may be more important than many tangible assets. Organizations need to protect sensitive or proprietary information—including information about the functions of the organization and its employees—as well as critical processes such as power generation, water purification, or financial transfers. For each individual asset, identify undesirable events and the effect that the loss, damage, or destruction of that asset would have on the organization. The overall value of the asset is based upon the severity of this effect. A worksheet is used to record the results of the Asset Assessment (see Table 1). Asset Assessment is the most important step of the risk management process as the next three steps build upon it.

Threat Assessment

In the Threat Assessment step, the security specialist focuses on the adversaries or events that can adversely affect the previously identified assets. The analyst or security specialist must replace intuition with a reliance on data and information obtained from research and interviews. As stated, the threat is considered in terms of adversaries. Common types of adversaries include criminals, business competitors, hackers, foreign intelligence services, terrorists, and others. In order to assess whether an adversary poses a threat the analyst or security specialist must determine if they have the *intent* and *capability* to cause an unwanted event and their *history* (proven track record) of successful attacks against the types of assets identified in Step 1. As above, information and automated processes must be considered.

Just as natural disasters and accidents are treated as threats even though they do not possess intent, cyber events (e.g. viruses and denial-of-service attacks) may also be treated as independent threats. Any organization that connects critical networks to the Internet must be aware of events in the larger environment. When short-term periods of intense politically-motivated protests take place, the infrastructure community can expect that it may be attacked, physically or via cyber means, regardless of the individual organization's involvement in the event being protested. Protesters often view utility companies as part of the government, regardless of whether they are privately operated. Companies or banks may also be attacked as symbols of globalization. Even protests between two foreign nations can spill over into the United States. Because the United States is a multicultural nation with a large global presence, U.S. organizations may suffer from attacks for any number of misguided reasons.

An efficient way for the analyst or security specialist to organize the threat data is by using a Threat Assessment Worksheet (see Table 2). This worksheet lists assets and undesirable events from the asset assessment worksheet. Each adversary that poses a threat to the organization's assets is listed next to each undesirable event that the adversary could cause. Next, the analyst enters what is known about the adversary's intent and capability to carry out the undesirable event. In addition, the analyst documents the adversary's history of causing the undesired event. The result is an overall threat level for that adversary. This worksheet allows the assessment information to be efficiently organized, documented, and later integrated into the complete analysis.

Vulnerability Assessment

The Vulnerability Assessment resembles the traditional security survey. In this step, the security specialist identifies and characterizes vulnerabilities related to specific assets or undesirable events. The security specialist is looking for exploitable situations created by lack of adequate security, personal behavior, commercial construction techniques, and insufficient security procedures. Examples of typical vulnerabilities include:

- The absence of guards
- Poor access controls
- Lack of stringent software or service contract review
- Unscreened visitors in secure areas

When designing and installing security systems security specialists should not count on vendors alone to build in appropriate levels of security. An assessment provided by an independent contractor that specializes in vulnerability surveys can provide the organization with an objective portrait of its vulnerabilities. It is essential that security specialist be, and stay, involved in the process—cradle to grave.

This step requires the security specialist to look at an asset from the outside inward as each of the potential adversaries might look at it. Specifically, the specialist should begin by studying the asset and asking questions such as: "If I wanted to physically harm this facility, I would…" or, "If I were a hacker, I would break into this by…" and so on down the list of adversaries and undesirable events. The severity of each vulnerability, when considered against the adversaries who might exploit them, and the assets they may attack, will then increase or decrease in importance. Therefore, the analyst or security specialist will be able to identify the relevant vulnerabilities most likely to be exploited by the adversary (see Table 3).

RISK = CONSEQUENCE × THREAT × VULNERABILITY

Risk Assessment

The Risk Assessment step is the point in the model where all of the earlier assessments (asset, threat, and vulnerability) are combined and evaluated in order to give a complete picture of the risks to an asset or group of assets. Using the worksheets in steps 1 through 3 the security specialist has arrived at individual category ratings by systematically analyzing the following questions:

- What is the likely effect if an identified asset is lost or harmed by one of the identified unwanted events?
- How likely is it that an adversary or adversaries can and will attack those identified assets?
- What are the most likely vulnerabilities that the adversary or adversaries will use to target the identified assets?

The purpose of this step is to evaluate how each of these ratings interacts to arrive at a level of risk for each asset. A risk analysis worksheet is extremely helpful in aligning all of this information into a readable and easily understood format that summarizes the previously collected information. Using the risk analysis worksheet (see Table 4) as a guide, the specialist should review all of the important factors associated with that single asset, referring back to the earlier worksheets and supporting data when necessary to understand how each increases or decreases the overall risk. By reviewing these ratings the specialist or analyst can begin to make an informed judgment of how "at risk" each asset is from its corresponding unwanted event(s). Looking across the worksheet, the analyst should be able to determine where the major vulnerabilities and threats lie, and compare risks across the spectrum of assets. At this point, an analyst is able to determine the major physical and cyber risks as well as which of these risks require immediate attention.

The terms used in the ratings may be imprecise. Although verbal ratings (low, medium, high, etc.) are subjective and hard to combine, they may be more comfortable to brief, depending on the audience. In situations where more precision is required, a numerical rating on a 1 to 10 scale can be used. A numerical scale is easier for an analyst to replicate and combine in an assessment with other scales.

A simple equation provides the underpinnings of the numerical system for rating risks and is expressed by the following: Risk = consequence × (threat × vulnerability). In this formula the "threat × vulnerability" segment represents the probability of the unwanted event occurring, and the "loss effect" represents the consequence of the loss of the asset to the organization.

When the needs of the *risk acceptance authority* (the person with the authority, financial and organizational, to reduce, retain, or transfer the risks identified on behalf of the organization) require only an assessment of risk to an asset, some analyses will end at this point. In most cases, however, the analyst will also recommend countermeasures or other options to the risk acceptance authority. In such cases, the following step is also included in the Risk Management Model.

Identification of Countermeasure Options

The objective of identifying countermeasure options is to provide the risk acceptance authority with countermeasures, or groups of countermeasures, which will lower the overall risk to the asset at an acceptable level. Using the risk analysis worksheet as a guide, the security specialist can identify which vulnerabilities need to be addressed. By evaluating the effectiveness of possible countermeasures against specific adversaries, he or she will determine the most cost-effective options. In presenting countermeasures to the risk acceptance authority, the security specialist should provide at least two countermeasure packages as options. Each option should also include the expected costs and amount of risk that the decision-maker would accept by selecting a particular option. A word of caution, if the wrong choice is made by selecting option B instead of option A, for example to cut costs, option B may not be the best choice in the long run. Upon conducting a consequence management assessment it may be found that, although initially more expensive, option A would save money whereas option B would actually lead to loosing money or critical data. This completes the risk analysis task and allows the decision-maker to make a sound risk management decision for the present time.

Continuous Assessment[3]

This model is a continuous process and not intended to result in a one-time "snapshot" of an organization's risk profile. Organizations that embrace an intelligent approach to risk management will constantly monitor any changes in their assets, the threat, and their vulnerabilities, as well as the larger infrastructure of which the organization is an element. As changes appear, the analyst will return to the model, enter the changes, possibly arrive at a new risk assessment, and recommend new countermeasure options. The continuous nature of risk assessment allows organizations to develop a risk-aware culture that understands, validates, and implements the decisions of the risk acceptance authority and the resulting countermeasures. New threats will emerge, some from new sources, which may be low-tech as well as high-tech. The resulting risks may appear too quickly to be addressed in a traditional top-down fashion. Organizations using a process of continuous assessment will be better able to manage these new risks in a timely manner, and for a longer period of time.

Conclusion

Risk management is a systematic, analytical process to determine the likelihood that a threat will harm an asset or resource and to identify actions that reduce the risk and mitigate the consequences of an attack or event. Risk management principles acknowledge that while risk generally cannot be eliminated, enhancing protection from known or potential threats can reduce it. As described in this paper, a risk management approach has several elements: an assessment of assets, an assessment of threats, an assessment of vulnerabilities as well as countermeasures and continuous assessment. According to the

[3] Derived from material used by the Information Solutions Division of Veridian in presenting its course on Continuous Risk Management.

General Accounting Office (GAO), successful risk management organizations have senior management who support and are involved in the process, employ the concept of "Risk Acceptance Authority" and create procedures for establishing and tracking accountability. This general approach is used or endorsed by federal agencies, government commissions, and multinational corporations (GAO-02-208T Homeland Security). By following the steps in this risk management guide, the security specialist and asset stakeholder can assess physical and cyber risks to their organization and address them appropriately. Furthermore, this reduction in their organization's overall risk can be accomplished in an efficient and cost-effective manner.

This product was completed with support from the CRUCIAL PLAYER project. CRUCIAL PLAYER is an interagency project initiated in 1999 by the Deputy Secretary of the Department of Defense (DoD), the Deputy Director of the Federal Bureau of Investigation (FBI), and the Deputy Director of the Central Intelligence Agency, and funded by DoD and FBI. The project is managed by the National Infrastructure Protection Center, Washington D.C. Major contributions to this product were made by Ed Jopeck, Paul Ruehs, and Scott Curthoys. Forward comments or questions to NIPC at 202-324-2084.

Table 1: Asset Assessment Worksheet with Examples

Assets	Undesirable events	Loss assessment
Key personnel	Loss of availability due to injury or death	High
File server	Loss of availability due to power disruption	Critical
Customer data	Loss of confidentiality due to unauthorized insider access	High
Principal Production Facility	Loss of availability due to natural disaster	Critical
Pipeline	Loss of availability due to sabotage	Medium

Table 2: Threat Assessment Worksheet with Examples

Assets	Undesirable events	Adversary	Intent	Capability	History	Threat level
Key personnel	Loss of availability due to injury or death	Criminals and Terrorists	Yes	Yes	Infrequent	Low
File server	Loss of availability due to power disruption	Nearby construction	N/A	Yes	Yes, at nearby locations	Medium
Customer data	Loss of confidentiality due to unauthorized insider access	Unchecked services subcontractor with access to network	No	Yes	No	Low
Principal Production Facility	Loss of availability due to natural disaster	Earthquake	N/A	Yes	Intermittent	Medium
Pipeline	Loss of availability due to sabotage	Protestors	Yes	Yes	Frequent	High

Table 3: Vulnerability Assessment Worksheet with Examples

Assets	Undesirable events	Vulnerabilities	Existing countermeasures	Vulnerability level
Key personnel	Loss of availability due to injury or death	No access controls to building, no central alarm system, unclear emergency succession plan	Single locks on doors, multiple alarm systems.	Medium
File server	Loss of availability due to power disruption	Extensive construction in area; Frequent violent storms in Summer	Batteries	Medium
Customer data	Loss of confidentiality due to unauthorized insider	Service to network done by unchecked subcontractor with root access	None	High
Principal Production Facility	Loss of availability due to natural disaster	Main building not strengthened, Water and electricity lines not hardened	Generator building constructed to standard	Medium-high
Pipeline	Loss of availability due to sabotage	No access control over entire length, numerous pumping stations, no roving guard force	Security guard at night at pump stations	High

Table 4: Risk Analysis Worksheet with Examples

Assets	Undesirable events	Loss Effect	Threat	Vulnerability	Countermeasure options	Risk
Key personnel	Loss of availability due to injury or death	High	Low	Medium	Central access control and alarm system, security guard, new emergency succession plan	Low
File server	Loss of availability due to power disruption	Critical	Medium	Medium	On-site generator Redundant management server off-site	Medium-low
Customer data	Loss of confidentiality due to unauthorized insider	High	Low	High	Monitor user log Tightly constrained user privileges	Low
Principal Production Facility	Loss of availability due to natural disaster	Critical	Medium	Medium-high	Retrofit earthquake proofing to main building, on-site water storage	Low
Pipeline	Loss of availability due to sabotage	Medium	High	High	24-hour security guard at pump stations, aerial patrols, CCTV	Medium