6.3 Threat Assessment

Threats are the likelihood of, or potential for, hazardous events occurring. They can affect any asset or object on which an enterprise places value. An enterprise threat assessment identifies the threats posed to the enterprise's assets, and determines the likelihood or frequency of their occurrence.

Example

The museum has begun a risk assessment and identified the following assets to be in scope:

Information asset types

- Museum employee data
- Museum financial/insurance data, partner financial data
- Museum contractual data and business planning
- Museum research and associated data
- Museum advertisements and other public data
- Museum database of collections information

Physical Assets

- Museum building
- Museum staff
- Museum collections and exhibits
- Museum transport vehicles

The museum has also identified the major security needs for these assets using SECURITY NEEDS IDENTIFICATION FOR ENTERPRISE ASSETS (89), and must now determine the threats to those assets.

Context

An enterprise has defined the assets to be included in a risk assessment and must now identify the events that could cause harm to those assets.

Problem

Enterprise assets face a barrage of attacks and hazardous events from all directions. Without effectively acknowledging the origins and frequency of these threats, an enterprise may never recognize the extent to which their assets are at risk.

How can an enterprise identify harmful events and determine the likelihood of their occurrence?

An enterprise must resolve the following forces:

- It must identify only those threats that have the potential for causing damage
- The type of business in which an enterprise is engaged will strongly affect the potential threat sources it will face
- The enterprise would like to develop a standardized way of identifying threats and assessing their likelihood, to be consistent with subsequent threat assessments
- The solution should address all assets included in the scope of a risk assessment, including informational and physical assets and, ideally, should be able to address vulnerabilities in non-IT systems

Solution

Systematically and explicitly identify and assess the threats against an enterprise and determine the types of protection they need. This activity is typically performed by an enterprise architect or strategic planner, and includes the following steps:

1. Identifying threats.

   Identify major threat sources that could potentially impact the assets defined by the scope of the risk assessment and trace their threat actions and consequences.

2. Building a threat table.

   Build a threat table by grouping threats first by asset type, then threat source.

3. Creating a likelihood scale.

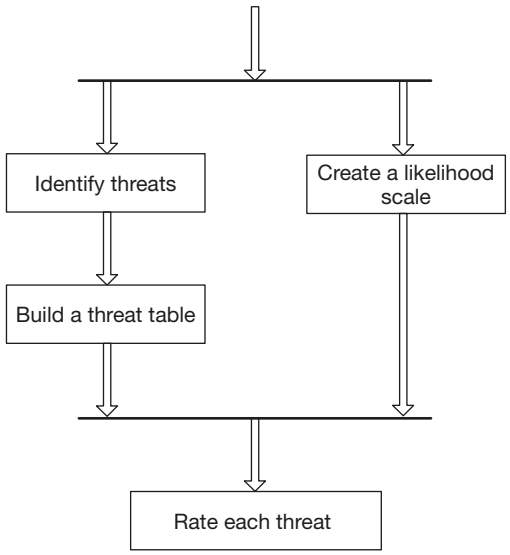
   Create a scale for rating the frequency of attempted events, or likelihood for events occurring. This scale will represent the expected rate of occurrence of a given hazardous (natural or accidental) event, or an attack attempt.

4. Rating each threat.

   Rate each threat according to the likelihood scale, and update the threat table to reflect this rating.

Dynamics

First, identify threats to the assets define by the scope of the risk assessment and build a threat table. A threat likelihood scale can also be developed in parallel. Finally, using the severity scale, rate each threat and update the threat table. The allowable sequence for performing a threat assessment is shown in the figure below.



Threat assessment sequence constraints

Implementation

The implementation of the process for assessing threats is described below.

1. Identifying threats.

   A threat consists of three parts: the threat source, action and consequence.

   - The threat source is that which initiates an attack or causes an event: a youth, an employee, or a fire, for example.
   - The threat action is the specific method by which an attack or event is carried out. An e-mail worm, a careless command entry, or water short-circuiting a motherboard are examples of threat actions.
   - The threat consequence is the security violation that results from the successful realization of the harmful event. Disruption of service, exposure of data, or destruction of hardware are some examples of the consequences that may occur.

Commonly, the threat source and threat action are grouped together and referred to as simply a 'threat.'

When determining threats it is only necessary to consider those that are relevant to the assets, as defined by the scope of the risk assessment. Similarly, when an infrastructure is modified, such as when new applications are installed or new communication paths created, this threat landscape will change. Guidelines for defining the threat landscape include the following:

- Specific environmental threats can quickly be removed given geographical or geological situations. For example, earthquakes cannot occur where there is no tectonic collision, tsunamis can only reach so far inland—although a flood can certainly occur in a building with a water supply.
- Threats that have no measurable chance of occurring within the life expectancy of an asset can be eliminated. Forms of material decay or deterioration, or astronomical hazards—while all being possible—have such a low frequency of occurrence that they can realistically be ignored.
- Threats can only target vulnerabilities. If a system isn't vulnerable to an exploit, then there is no threat, and consequently no risk. Consider a network environment consisting solely of Unix machines. Attacks launched against that network exploiting a buffer overflow on a Microsoft IIS Web server will obviously be ineffective, and thus the threat landscape should not include these threats.
- Alterations to the management of data or other enterprise assets will alter the threat landscape. An attack that was previously not possible may now exist. For example, providing remote VPN access to employees now exposes an enterprise to residential-based threats.

Threat sources

Sources of threats can be natural or human in origin. Natural threat sources are environmental forces frequently referred to as 'Acts of God.' Examples of natural threat sources include the following: tsunami, earthquakes, wind, snow, or rain storms.

Human threat sources can be deliberate (attacks) or accidental (errors). Deliberate human threat sources are attackers and are differentiated by their motives, capabilities, and the assets they target. Those who seek to deliberately cause harm include the following:

- Hackers. They are generally motivated by mischief or grandstanding and may only seek publicity or notoriety among their peers. They employ simple tools, often precompiled using point-and-click interfaces created by others. While the tools may not be sophisticated, the results can range from the minor annoyance of a defaced Web page to major damage caused by the mass dissemination of malware such as worms or viruses.

- Professional criminals. They are motivated by financial reward and thus may steal credit card numbers, personal health information (PHI) or specialized documents such as corporate trade secrets, blueprints or recipes, and offer them for sale to competitors, the corporation from which they were stolen, or the individuals themselves. Their techniques are more advanced than the youth hacker, both in organizational structure, technological skills and attack execution.
- Terrorists. They care little for Web page defacement, but more for infrastructure disruption and destruction. Their methods can be crude but highly effective. The targets can be civilian, diplomatic, or military personnel in addition to public infrastructure systems such as power generation and distribution, water processing, telecommunications, financial/banking, emergency services, or transportation systems. Terrorist groups are often well funded and highly organized.
- Internal threat. Current or past employees who are angry or disgruntled are motivated by revenge or anger. They know the assets and the defences of an organization, and can destroy data or interrupt services, posing a serious threat to any enterprise.

Accidental threat sources are actors who inadvertently cause damage or compromise the security posture of an asset. They may be employees or customers who are careless, inattentive or poorly-trained. This form of threat source might also be an application that is simply performing as programmed and mistakenly compromises a system.

Threat actions

Threat actions are the actual events that exploit the weakness of a system. They are the methods used by attackers to gain control of assets, they are the naturally-occurring events that cause damage to systems, and they are the mistakes made by negligent users. They fall into the following categories:

- Natural. This includes extremes or fluctuations in temperature, causing metal fatigue or structural distress, electrical failures, surges, spikes or brownouts, fires, as well as natural disasters such as lightning strikes, earthquakes, uncontrolled flow of water into buildings or rooms through. rain, floods, inundation, storms or hurricanes.
- Human deliberate. An example might be an attacker masquerading as a system administrator, using social engineering techniques to gather personal information about users, or an employee planting a logic bomb in a system, scheduled to erase critical system files.
- Human accidental. For example, a data center employee who inadvertently stumbles and jerks the power cord from a production server, or an employee

transferring a file from a personal laptop to a corporate desktop, unaware that the file is infected with a virus.

Threat consequences

The realization of a threat can result in the violation of one or more of the security properties defined throughout this book: confidentiality, integrity, availability, or accountability. Regardless of the source or action of the threat, the consequences will be one of disclosure, deception, disruption, or usurpation, as discussed by the security violations in Chapter 2.

2. Building a threat table.

   Grouping by asset type becomes useful when the final risk to each asset is determined. Further grouping by threat source ensures that one does not overlook the fact that the same threat action can be initiated by different sources, each with a corresponding, and possibly different, frequency. For example, theft can occur from both a professional criminal and an employee. However, the frequency of theft from employees may be significantly higher than that of a criminal.

   The threat consequence is included for each threat action, and provides supporting clarification of the possible outcome of an incident.

   It is possible that the threat table will be updated after the completion of the vulnerability assessment. Given the tight relationship between threats and vulnerabilities, identification of vulnerabilities can lead to the discovery of new threats that were previously not considered.

3. Creating a likelihood scale.

   While difficult to determine in precise quantitative terms, qualitative values can be used and numeric estimates can be correlated. As an example, Table 6.13 shows a modified version of the probability levels given by [Herr02].

Table 6.13 Event likelihood

RATING	LIKELIHOOD	DESCRIPTION
6	Extreme	The threat action is continually occurring
5	Very high	The threat action occurs very often
4	High	The threat action regularly happens
3	Medium	The threat action occurs infrequently
2	Low	This threat action rarely takes place
1	Negligible	The occurrence of this threat action is extremely unlikely within a human lifetime

Note that this table does not represent the only way to categorize event frequencies. Other threat assessments methodologies exist that define their own scale and they are equally valid. The important point is that an enterprise use the same scale year after year, to provide consistent results between assessments.

4. Rating each threat.

   Each threat will have a certain likelihood or frequency of occurrence, and as expected, some will transpire more often than others, based on specific factors. Note that this is not the frequency of successful violations in which damage has occurred, but an event or attack that could cause damage.

   To estimate or predict the frequency of a threat, it is necessary to consider many issues. Factors that affect the likelihood of a natural threat include the following:

   - Proximity to dangerous chemical or petroleum factories. A few additional miles from an industrial incident may make the difference between a precautionary evacuation of a facility and human fatalities.
   - The possibility of extreme weather patterns and fluctuations such as heat, wind, rain. While internal temperatures can be controlled to a certain degree, external temperatures can overload the control systems, affecting both human and mechanical systems. Specific geographical locations will naturally be more prone to such fluctuations and extremes.
   - The state of the operating facilities with regard to structural integrity, fire suppression, and other emergency response systems. Older, less sturdy buildings may require constant refurbishment, resulting in disruption of service.

   Factors that affect the likelihood of a deliberate human threat include:

   - The time since a vulnerability has been publicly known. The longer since the vulnerability has been discovered, the greater the number of attackers that will be aware of it, and the more opportunity there will be to catalog, research and develop tools to exploit it.
   - Whether or not a working exploit is available for the vulnerability. Graphical user and command-line interface exploits certainly have a much greater chance of being used than ones that require custom development such as coding. Having precompiled or point-and-click code reduces the knowledge level required to launch an attack: suddenly, one does not need detailed knowledge of the vulnerability in order to exploit it.
   - The frequency of attack attempts. The more frequent the number of attack attempts, the greater the chance of a successful attack.
   - The potential reward offered to an attacker. Hacker challenges and monetary reward increase the chances of an attack.

- The asset value. High-wealth businesses and assets attract more attention than those of lesser value, and therefore offer more incentive for compromise. Attackers will therefore not generally target systems that contain no value, or provide no reward. There are two exceptions to this, however: either an attacker targets the system out of curiosity or simply to prove that it can be done, or an attacker breaches a useless system only to provide a launching point to another system of value (for example, compromising a home computer in order to penetrate a corporate network).
- The perceived difficulty of realizing a successful attack. If the asset is known to be heavily protected and the chances of reward low, the fewer will be the number of attempts.
- Public visibility and sentiment towards the business. Organizations that are viewed as having an unpopular affiliation, or that act inappropriately, may incur more attacks as a result.
- Employee morale. Low employee morale frustrates employees and can cause malicious or vengeful retaliation. It can also simply cause indifference to quality and service. Either way, low morale increases the potential for accidental or deliberate threat actions.
- Past prosecutions. If an organization is known for seeking retribution and prosecution of crimes, attackers will seek easier or less risky targets.

Factors that affect the likelihood of an accidental human threat include:

- The availability of skilled employees. If unqualified personnel are required to manage sensitive or complex systems, the opportunity for errors due to ignorance or mistakes increases greatly.
- Security measures. Administrative controls, such as user awareness and emergency training, educates users on policies and procedures, making them less susceptible to social engineering attacks and more aware of information security requirements.
- The frequency of changes to systems, including patches, upgrades, and other modifications. The more frequently changes are made, the more potential there will be for mistakes or corruption due to new configurations.

Arguably the most reliable method for determining the frequency of future events is historical data. Naturally-occurring events are often recorded by educational and governmental organizations for study. Commercial and governmental references exist that record information security attacks. Relevant data can also be collected from the enterprise's own systems. Some examples of useful sources include the following:

- Historical almanacs (in the cases of natural disasters).
- News archives including federal services. For example `http://www.fema.gov/`

- Information security newsletters and Web sites. For example, `http://www.securityfocus.com`, CERT, Symantec, FedCIRC and SANS.
- Current and archived intrusion detection, incident response and application system log files.
- Previous threat assessment documents, if available, may also contain particularly relevant information.

Example Resolved

From SECURITY NEEDS IDENTIFICATION FOR ENTERPRISE ASSETS (89), the museum has identified its informational and physical assets:

Information Asset Types

- Museum employee data
- Museum financial/insurance data, partner financial data
- Museum contractual data and business planning
- Museum research and associated data
- Museum advertisements and other public data
- Museum database of collections information

Physical Assets

- Museum building
- Museum staff
- Museum collections and exhibits
- Museum transport vehicles

After use of THREAT ASSESSMENT (113), the museum has identified a brief list of threats to information and physical assets, as shown in the threat Tables 6.14 and 6.15, respectively.

Known Uses

Threat assessment is, for example, defined in the ISO Technical Report 13335-3 [ISO13335-3]. This definition of the process focuses on three tasks: identification of threat sources, the threat target, and the threat likelihood. It identifies that determining the likelihood should take into account the threat frequency, the threat motive and geographical factors such as proximity to industrial factories. This technical report differentiates the threat likelihood simply as high, medium and low. The actual determination and definition is left to the implementer of the threat-assessment process.

Table 6.14 Threats to information assets

THREAT ACTION (FREQUENCY)	THREAT CONSEQUENCE
Natural	
Electrical spike in computer room (3)	Incapacitation, corruption of informational assets
Loss of electronic documents (3)	Incapacitation of informational assets
Professional criminals	
Theft of information assets (3)	Misappropriation, incapacitation, misuse, exposure, corruption of informational assets
Employees	
Unauthorized access to informational assets (5)	Exposure, falsification, incapacitation, misappropriation of informational assets
Data entry errors (5)	Corruption of information assets
Leaking confidential information (3)	Exposure of information assets

Table 6.15 Threats to physical assets

THREAT ACTION (FREQUENCY)	THREAT CONSEQUENCE
Natural	
Museum fire (3)	Incapacitation of physical assets
Fatigue of support fixtures, building structural failure (3)	Incapacitation of physical assets
Failure of monitoring and alarming systems (4)	Intrusion, misappropriation of physical assets
Professional criminals	
Theft of museum collections and exhibits (2)	Misappropriation of museum collections and exhibits
Physical attack against employees (3)	Incapacitation of employees

Table 6.15 Threats to physical assets (*continued*)

THREAT ACTION (FREQUENCY)	THREAT CONSEQUENCE
Employees	
Accidental damage to museum collections and exhibits (4)	Incapacitation of museum collections and exhibits
Accidental damage to vehicles (4)	Incapacitation of museum collections and exhibits
Theft of museum collections and exhibits (2)	Misappropriation of museum collections and exhibits
Misconfiguration of monitoring and alarm systems (4)	Incapacitation, obstruction of monitoring and alarm systems
Museum patrons	
Accidental damage to museum collections and exhibits (3)	Incapacitation of museum collections and exhibits

NIST also describes a complete risk management process whose first step is a risk assessment [NIST800-30]. Steps 3.2 and 3.5 in this process are dedicated to the identification of threats and determination of their likelihood. This publication also uses a likelihood scale of high, medium and low. In making the determination of the likelihood of a threat, this scale also incorporates the existing controls and their capability to neutralize the threat. NIST also separates the identification of threats and the likelihood of their realization into two separate processes.

In her publication *Security Engineering and Information Assurance*, Debra Hermann describes the need for a complete information security process to identify threats, their type, source, and likelihood [Herr02].

Microsoft describes a threat and countermeasures pattern that offers alternative methods for identifying and assessing threats through 'Threat Modeling' [Mei03]. The authors use a method called STRIDE that categorizes threats based on the 'goals and purposes of the attacks.' The categories that make up the acronym are: spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privileges.

Consequences

This pattern has the following benefits:

- The solution provides the enterprise with an understanding of the factors that increase both the existence and the frequency of harmful events.
- It identifies the consequences incurred should a given threat be realized.
- The threat assessment is a major component of the risk assessment pattern set that will prioritize and ultimately result in a more secure organization.

It also has the following liabilities:

- Accurate historical data may not be available, preventing the enterprise from acquiring useful threat frequency data.
- The effort required to conceive of all possible threats can be too time consuming for an enterprise. Constraints may therefore have to be placed on the completeness of the threat landscape.