

This second module covers the following topics:

Risk and Impact

Assets and Categories

Risk Assessment and Analysis

Risk Management



Instructional Objectives

- Discuss the components of risk and the concepts of risk management
- Describe the importance of identifying and prioritizing assets
- Describe risk analysis techniques
- Identify methods of managing risks

The purpose of this module is to familiarize the students with risk and asset management. To do this, the students must have an understanding of the key attributes of risk and the concepts of risk management (including risk analysis assessment). One of the key attributes introduced is the valuation and determination of assets. In most organizations, identifying and prioritizing assets based on their value, cost, or importance constitute this valuation and determination process. This module focuses on organizations that select and prioritize assets based on the asset's importance or relevance in fulfilling the mission and objectives of the organization.



Overview

Define risk and recognize impact

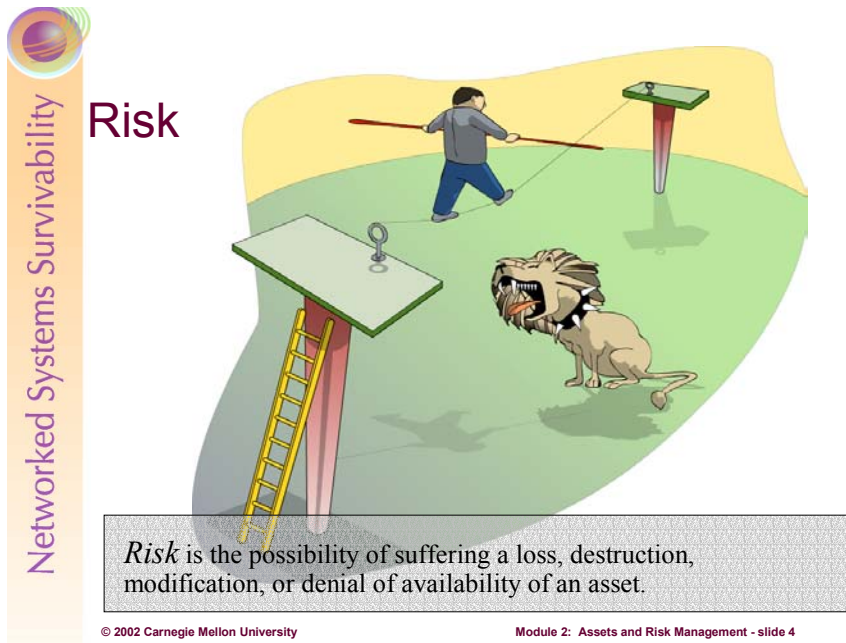
Assets, threats, vulnerabilities and safeguards

Risk management, risk assessment and analysis

© 2002 Carnegie Mellon University

Module 2: Assets and Risk Management - slide 3

This module introduces concepts and applications of risk management (including principles, attributes, and activities). At a conceptual and educational level, this section explains risk, risk impact, risk attributes, assets, asset categories, risk analysis and risk management. Additionally, this section also examines the application of risk management. This examination will include the description of risk assessment and analysis activities, comprehension of the impact of risk events, and recognition of mitigation strategies for managing and reducing risk.

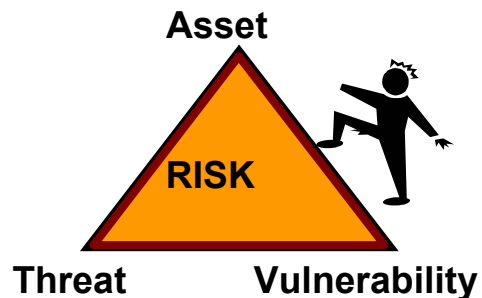


Description of Risk

Risk is the possibility of suffering harm or loss. With respect to information and computer data, risk is the possibility of suffering a loss (or impact) due to disclosure, destruction, modification, or denial of service of the information. These outcomes of risk directly affect the properties of confidentiality, integrity, and availability of the information as well as information survivability and security.

For a risk to exist, the following must be present:

- Assets of value to an organization or individual that must be protected (critical assets)
- Threats to these critical assets (possibility of disclosure, modification, destruction, or interruption)
- Vulnerabilities of the critical assets that may provide an opportunity for threats to act on the asset in a manner that discloses, modifies, destroys, or interrupts the asset



Before risks can be managed, they must be identified. One way to examine for potential risk is to list the components of risk in an asset-driven scenario and gauge the risk's plausibility.

Example of Risk

For example, let's consider a home user making a consumer purchase over the Internet. In this situation, the user must submit customer information to the Web site (i.e., item, quantity, name of customer, address of customer, payment type, credit card number, etc.) to complete the purchase. Therefore from the user's point of view (even if he or she is not explicitly aware of the risk or is seemingly unconcerned), risk certainly exists. To identify the risk in this situation, we can state that the asset is the customer's information, the threat is anyone on the Internet with malicious intent, and the vulnerability is any technology weakness that allows the information to be observed and captured.

Qualitative and Quantitative Measures of Risk

Risks are traditionally captured as a description that can then be measured both qualitatively and quantitatively. Again, let's use the example above to demonstrate this point. Qualifying the risk in the scenario means understanding the negative impact with respect to the asset as well as the likelihood of the threat. This impact occurs when the asset is destroyed, modified, interrupted, or disclosed. To the home user, qualifying the risk means looking at the result of having their personal information disclosed and the impact. In this case, the users will probably be most concerned with their financial liability, identity loss, and laws and regulations to which they may be subjected, as established by a qualitative scale (or criteria) for evaluating the risk (such as high, medium, or low).

Quantifying the risk means understanding the possibility of the risk existing or coming to fruition. Here the home user attempts to measure the probability or likelihood of someone performing several different attacks whose goals are to retrieve his or her personal information. This measurement takes into account questions such as the following:

- How likely is it that someone may observe the information in transit between the home user and the website (and possibly decode the encrypted network traffic)?
- How likely is it that the software making the exchange of personal information is vulnerable to attack?
- How likely is it to be singled out as a victim over all of the other Web commerce transactions happening at the Web site of purchase?
- How likely is it that an attacker might gain access to the information once it has arrived at the website?

These are just a small sample of the risks involved in this simple transaction. For the individual to really understand these risks, he or she must appreciate the potential impact of these risks. This demands an understanding of the potential that threat sources (humans, system problems, viruses, etc.) have in exploiting and abusing vulnerabilities that result in risk. This potential falls into a continuum ranging from negligible to actual, over the life of the information being transmitted, stored, and processed.

Threats and Vulnerabilities

Probably the most readily identifiable components of risk, to system and network administrators, are threat and vulnerability. The combination of threat and vulnerability yield a potential for undesirable outcomes that affect assets. The loss or impact of an event (caused by inappropriate, accidental, or negligent means) results from threats and the exploited vulnerabilities creating an outcome of disclosure, modification, destruction, or interruption of an asset.

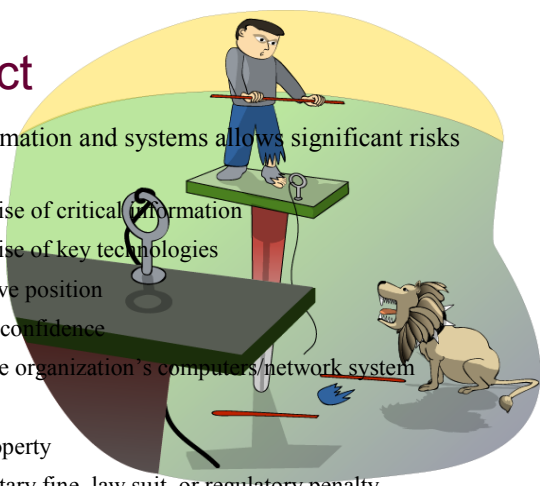
The concepts of threat and vulnerability were briefly introduced in Module 1 -- Challenges to Survivability. Having knowledge that threats and vulnerabilities are components of risk is adequate for our current discussion of risk management concepts and principles. However, since risk management, in practice, often requires more detail and knowledge of specific vulnerabilities, threats, and threat actors, this information will be discussed further in Module 8 -- Threats, Vulnerabilities, and Attacks.

Networked Systems Survivability

Risk Impact

The nature of information and systems allows significant risks that may result in:

- Loss or compromise of critical information
- Loss or compromise of key technologies
- Loss of competitive position
- Loss of customer confidence
- Loss of trust in the organization's computers/network system
- Loss of revenue
- Loss of life or property
- Loss due to monetary fine, law suit, or regulatory penalty



© 2002 Carnegie Mellon University

Module 2: Assets and Risk Management - slide 5

Understanding a risk's impact forms the basis for evaluating outcomes of risk: loss, destruction, modification, and interruption. Impact is the actualization of a risk. To evaluate the outcome of a risk, we start by developing evaluation criteria for risk scenarios.

For example, let's consider a home user who sets up a personal Web server to display his or her resume. As a risk management process, our home user will identify his or her assets, consider the possible negative outcomes, and characterize the impact of an asset's failure. Here, our home user recognizes that one asset, for example, is the Web server itself while another is his or her resume. Using the resume in this example, the possible negative outcomes to the *information asset* include:

- Destruction of the resume file
- Modification of the resume content
- Pirating the resume data
- Interruption of its presentation to the Internet

If we consider the potential negative impact due to these conditions actually occurring, our home user should be able to define potential failure conditions, such as:

- Destruction, causing an expenditure of effort to restore or recover the information
- Modification, causing a prospective employer to consider the candidate either adequate or inadequate for the position, depending on what information was changed
- Theft, causing a loss of creative and competitive marketing of the individual's skills or background
- Interruption, causing an inability for potential employers to view the candidate's information

Finally, the home user must evaluate the impacts, deciding whether he or she really cares about the potential impacts to the assets involved. If yes, then mitigation strategies should be supplied; if no, then the potential risk impacts are accepted in addition to the consequences of loss or harm suffered through the risk.

Understanding Risk

Requires:

- Identifying and prioritizing assets
- Relating threats and vulnerabilities
- Performing risk analysis
- Recognizing risk must be managed

Risk can be mitigated, but cannot be eliminated

Identifying assets involves a discussion within the organization to determine what categories of assets exist, who owns each asset, and what level of protection is necessary for the asset. This exchange of information should happen between the managers, staff, and information technology personnel on a periodic basis and as part of the organization's review of its information security policy. These events are an important component for identifying assets and risk mitigation plans because they enable the organization to identify its current protection strategy for each asset and any changes to the asset's priority with respect to different levels of the organization. This priority discussion allows a ranking of one asset over others, and it should be documented and reflected in organizational policy, recognizing that assets may be mission critical, non-critical but sensitive, or general in nature.

Relating threats and vulnerabilities to an asset is part of a risk assessment activity, discussed later in this module, and requires that those who are responsible for protecting the information assets have an appreciation of the range of threats and vulnerabilities. Once the range is known, the likelihood of any one threat acting adversely on an asset must be understood.

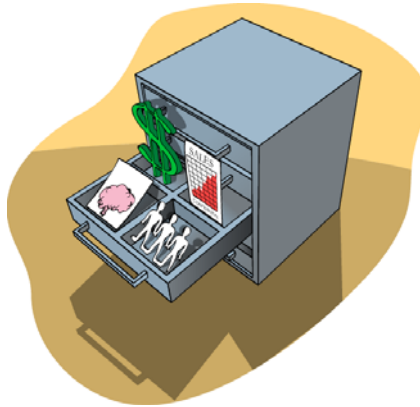
The results of risk analysis identify the strategies (plans, policies, technological mechanisms) that will help to mitigate the risk. Analysis includes evaluating the risk to an organization and measuring that risk against the impact to the organization if an event occurs. For example, a determined risk for a medical organization may be that "modification of paper medical records by unauthorized individuals can lead to loss of life, financial or punitive penalties, or loss of customer confidence." This risk is actually stated as a risk scenario that embodies the properties of assets (paper medical records), threat actor (personnel exceeding their privileges or unauthorized outsiders), outcome (modification of the records), and impact (public safety, financial, customer confidence, legal). Risk analysis determines which risks are viable (that is, non-negligible) and what degree (high, medium, or low) the impact has on the organization when evaluated.



Assets

Assets and asset value

- Information Assets
- Other supporting assets
- Critical assets



© 2002 Carnegie Mellon University

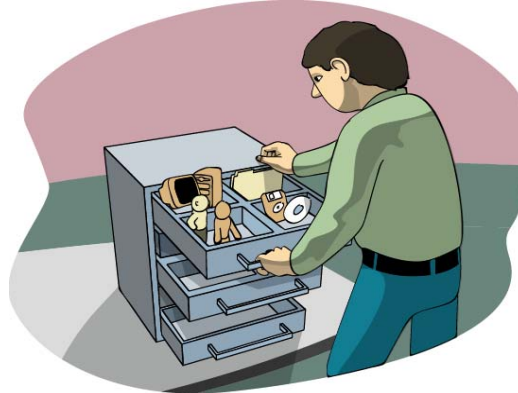
Module 2: Assets and Risk Management - slide 7

An asset is anything of value to the organization. Typically, assets fall within categories of information assets (people, hardware, software, systems), other supporting assets (facilities, utilities, services), and critical assets. Critical assets may include information or other supporting assets. In the following sections, we will describe examples within each category.

It is important to note that your organization may choose to classify assets within different categories according to sensitivity or function. Asset definitions may be highly subjective and asset value even more so; therefore, an easier way to approach assets and asset value can be to consider the worth of the asset (in both tangible and intangible aspects) to the organization. By examining the costs associated with the value and intrinsic value of an asset (qualities of the asset's existence), you may discover a more meaningful definition and value of the asset.

Information Assets

Information
Hardware
Software
People



© 2002 Carnegie Mellon University

Module 2: Assets and Risk Management - slide 8

Information includes:

- Data being processed on, stored on, or transmitted between systems
- Backup and archive data (on-site and off-site storage volumes and locations)
- Paper documents
- Escrowed encryption keys
- Software distribution media

Hardware includes:

- Desktop computers
- Servers
- Mainframes
- Network equipment (routers, switches, firewalls)
- Wiring infrastructure
- Wireless support infrastructure

Software includes:

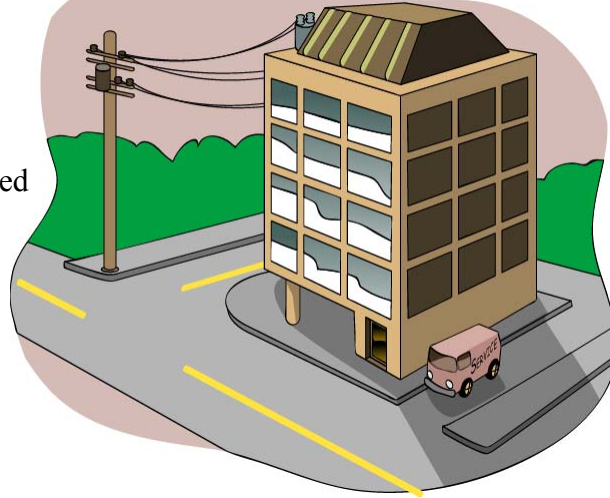
- Commercial off-the-shelf (COTS) software
 - Operating systems
 - Desktop software
 - Mainframe applications
- Custom software
 - In-house effort
 - Outsourced effort
 - Ad hoc scripts
- Undocumented tools used by employees

People include:

- Senior and middle management
- Technical and non-technical staff
- Public relations
- Help desk, facilities, security
- Contractors, third parties (Computer Security Incidence Response Teams [CSIRTs])
- Government, police, fire

Other Supporting Assets

Facilities
Utilities
Outsourced
Services



© 2002 Carnegie Mellon University

Module 2: Assets and Risk Management - slide 9

Facilities include:

- Heating/ventilation/air conditioning (HVAC) support
- Power
- Water
- Telephone
- Security

Utilities include:

- Power
- Water
- Telephone
 - Leased lines (T1, T3, ISDN)
 - Voice lines
 - Cell phones
- Pager services
- Service level agreements
 - Hardware maintenance
 - HVAC support

Outsourced services include:

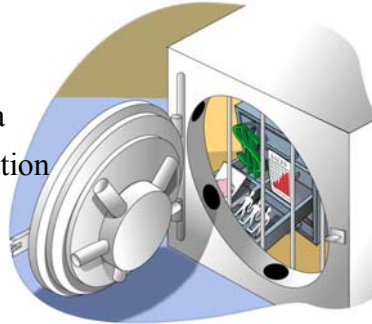
- Off-site services
 - Information storage
 - Web services
- Consultants
- Utilities
- Legal services
- Public relations
- Managed or monitored security
 - Physical
 - Network

Critical Assets

Critical Assets are assets determined to have an integral relationship with the mission of the organization and its success; recognizing that each individual organization will define a different set.

Examples:

- Intellectual property / patents / copyrights
- Corporate financial data
- Customer sales information
- Human resource information



© 2002 Carnegie Mellon University

Module 2: Assets and Risk Management - slide 10

Critical assets are assets that have an integral relationship with the mission of the organization. This means that loss or damage to a critical asset would cause disruption to the operational or functional mission of the organization to a point where the mission fails. This concept recognizes that each individual organization will define a different and unique set of critical assets that align with mission success or failure.

Examples of critical assets include:

- Intellectual property
 - Patents, copyrights
 - Software code under development
 - Systems acquisition or development projects
- Corporate financial data
 - Payroll information by employee, department, organization
 - Financial earnings, revenue, and loss statements
 - Stock dividend information
- Customer sales information
 - Names, addresses, credit card / account numbers, purchase histories, demographic information
- Human resource information
 - Names of employees, departments, salaries
 - Hiring, administrative punishment, and disability information
- Network architecture information
 - Network topology diagrams
 - Desktop or systems replacement plans
 - Strategic infrastructure plans
 - Vulnerability assessment reports
 - Types and locations of infrastructure (general purpose, storage, server, networking, and security devices)
- U.S. Government or military classified information
 - Compartmentalized projects
 - Deployment and strategic plans
 - Intelligence information, logistic movements/support
 - Technical specifications on equipment, weapons, projects

Security Requirements

Each [critical] asset has different requirements of confidentiality, integrity, and availability, that should be:

- Communicated
- Detailed
- Documented



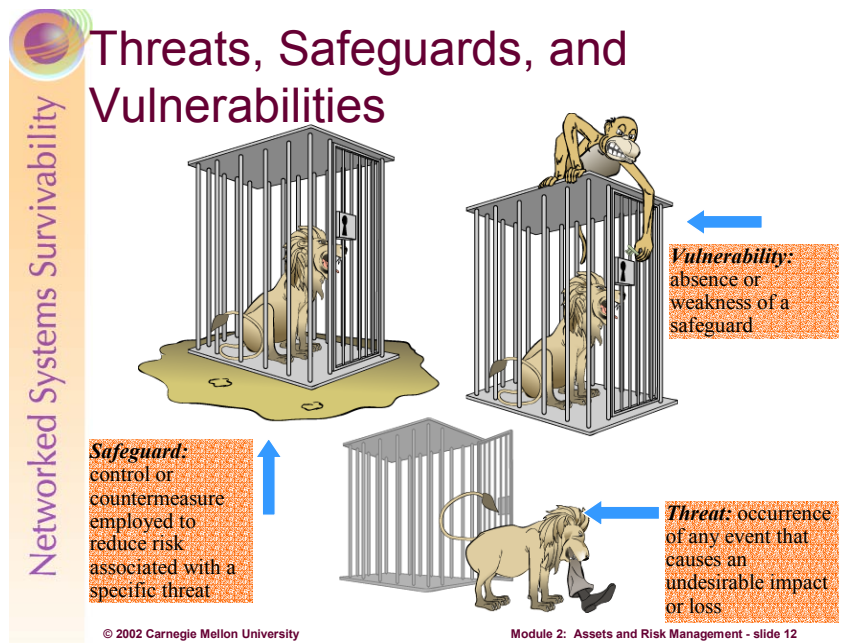
© 2002 Carnegie Mellon University

Module 2: Assets and Risk Management - slide 11

Each [critical] asset has different requirements of *confidentiality*, *integrity*, and *availability* that should be:

- Communicated throughout the organization, especially from the owner of the asset to the person(s) responsible for its safety and security
- Detailed, explaining under what conditions and to what degree the requirements must be enforced
- Documented, describing the requirements, the responsible owner(s), and party charged with its protection

Security requirements should be understood at all levels of the organization involved in the asset's protection. They should be described with enough detail for a specific requirement to be placed on the responsible owner (manager, user, system/security administrator, etc.) or the technology protecting the asset. They should be documented in security policies and plans.



Safeguards

A safeguard is the control or countermeasure employed to reduce the risk associated with a specific threat or group of threats as in the following examples:

- Access Control technologies
 - Firewalls
 - Access Control Lists on files and directories
 - Physical security systems like locks and card scanners
 - Encryption technologies
- Redundancy in systems
 - Clustered servers
 - Redundant sources of power and HVAC
 - Cross-utilization and training of IT personnel

Threats

A threat is any event that will cause an undesirable impact or loss to an organization if it occurs. Examples of threats include the following:

- Intrusions and disruptions to information systems
 - Viruses, Worms, and Trojan Horses
 - Denials of Service
 - Sniffing network traffic
 - Stealing data assets
- Loss of assets that are single points of failure
 - Critical data that is not backed up
 - Single, critical piece of network infrastructure (i.e. a core router)
 - Keys that are used to encrypt critical data

Vulnerabilities

A vulnerability is the absence or weakness of a safeguard. It can also be described as a weakness in an asset or the methods of ensuring that the asset is survivable. Examples of vulnerabilities include the following:

- Software and hardware flaws
 - Buffer overflows
 - Weak default configurations
 - Under-engineered hardware (i.e., not enough memory, disk space, etc.)
- Lack of policies and procedures
 - Undefined access controls
 - Lack of documentation
 - Users unaware of survivability issues

Networked Systems Survivability

Calculating Risk Exposure

Probability x **Severity** = **Exposure**

Use exposure values to:

- Prioritize the order in which risks are addressed
- Help in deciding how to manage risks

Risk	Probability	x Severity	= Exposure
A new worm attacks vulnerable systems	7	7	49
Web site defacement	2	8	16
Datacenter flooded by fire protection system	1	10	10

© 2002 Carnegie Mellon University Module 2: Assets and Risk Management - slide 13

Quantitative risk analysis can be a major project and can consume considerable organizational resources. It attempts to assign independently objective numeric values (hard dollars, for example) to the components of risk assessment and to the assessment of potential losses.

Qualitative risk analysis addresses more intangible values of loss, and typically attempts to produce scenarios so risk can be anticipated and managed. However, threat frequency and impact data is still required to conduct a qualitative risk analysis.

The above slide shows a simple exposure table that supports a qualitative risk analysis. Threat scenarios are described for assets (typically critical assets) and data from the exposure table is used for making decisions regarding risk management. The table also provides a starting point for determining which risks are of greatest concern when it comes to mission survivability. If a decision is made to mitigate the risk, typically a cost/benefit analysis is conducted to select safeguards.

Calculating Risk Where Metric = \$

Exposure Factor (EF)

- % of loss of an asset

Single Loss Expectancy (SLE)

- $EF \times \text{Value of asset in \$}$

Annualized Rate of Occurrence (ARO)

- A number representing frequency of occurrence of a threat
 - Example: 0.0 = Never 1000 = Occurs very often

Annualized Loss Expectancy (ALE)

- Dollar value derived from: $SLE \times ARO$



© 2002 Carnegie Mellon University

Module 2: Assets and Risk Management - slide 14

IT managers are often faced with the dilemma of justifying their expenditures when it comes to survivability and security. Early in this module we discussed the shift in thinking required such that resources allocated towards survivability should be seen as an investment (not a debit) when it comes to the mission of the organization. Because the old paradigm (security seen as an overhead expense) is still an operational reality, IT managers often justify expenditures with forms of quantitative risk analysis. The terms in the slide are pseudo-standards that help calculate risk in relation to actual dollar figures. Their usage helps to provide more reliable cost versus benefit analysis.

- **Exposure Factor (EF)**
The exposure factor describes the effects a threat event would have on a particular asset as a percentage of loss. For example, the loss of some hardware would have a small EF, whereas the catastrophic loss of all computing resources would have a large EF. The EF value is necessary to compute the Single Loss Expectancy (SLE), which in turn is necessary to compute the Annualized Loss Expectancy (ALE).
- **Single Loss Expectancy (SLE)**
The single loss expectancy is the dollar figure that is assigned to an organization's loss from a single threat event. It is derived from the formula $EF \times \text{asset value in dollars} = SLE$. For example, an asset valued at \$10,000 that is subjected to an exposure factor of 50 percent would yield an SLE of \$5,000.
- **Annualized Rate of Occurrence (ARO)**
The annualized rate of occurrence is a number that represents the estimated frequency with which a threat is expected to occur. This value can range from 0.0 (for threats that never occur) to a large number (for threats that occur frequently, such as misspellings of names in data entry). This number is usually created based upon the likelihood that the threat will occur and number of individuals that could cause it to occur. The loss incurred by this event is not a concern here, only how often it occurs. For example, an organization's data center being flooded by the fire control system could be estimated to occur once every 1000 years, and will have an ARO of .001. However, 100 help desk analysts making access control errors when administering accounts could be estimated at 15 times per year, resulting in an ARO of 1500.
- **Annualized Loss Expectancy (ALE)**
Annualized loss expectancy (ALE) is the annual financial loss an organization expects from a

Student Workbook – Module 2: Assets and Risk Management

threat. It is calculated by multiplying the single loss expectancy and annualized rate of occurrence ($SLE \times ARO = ALE$). For example, a threat with a dollar value of \$10,000 (SLE) that is expected to occur 5 times per year (ARO) will result in an ALE of \$50,000. [Krutz 2001]

Generally speaking, if an organization's information survivability expenditures are less than the sum of the calculated ALEs, then some quantitative return on investment (ROI) figures can be discerned.

Simple Risk Assessment Matrix

Asset = Organization's Intranet Web Server

Probability	High	Web page Content error		
	Medium		Web page Defacement	
	Low			Lightning Strike
		Low	Medium	High
	Severity			

© 2002 Carnegie Mellon University

Module 2: Assets and Risk Management - slide 15

Simple Risk Assessment Matrix

Even simpler than the exposure table is the above risk assessment matrix. It simply categorizes threats into levels of degree based upon the same probability vs. severity factors.

If a threat is in the High/High box in the matrix (high probability and high severity), an organization is likely to manage the risk associated with that threat first.



Detailed Risk Assessment Matrix

		Probability					
		Frequent	Likely	Occasional	Seldom	Unlikely	
		A	B	C	D	E	
SEVERITY	Catastrophic	I	1	2	6	8	12
	Critical	II	3	4	7	11	15
	Moderate	III	5	9	10	14	16
	Negligible	IV	13	17	18	19	20
		Risk Levels					

© 2002 Carnegie Mellon University

Module 2: Assets and Risk Management - slide 16

Detailed Risk Assessment Matrix

The above slide shows a more detailed risk assessment matrix (again based on the factors of probability and severity) that is used when making risk management decisions. Here, threats of varying probability are categorized in four levels of severity:

- Catastrophic – Complete mission failure
- Critical – Major mission degradation
- Moderate – Minor mission degradation
- Negligible – Less than minor mission degradation

The lower the risk level rating number, the more critical the risk is to the asset.

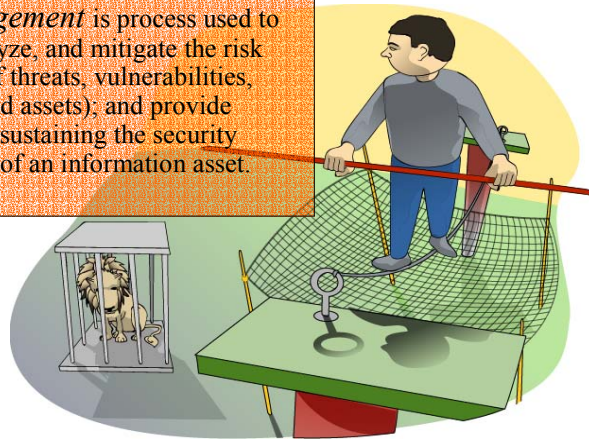
Summary of the Assessment Step

Risk is the probability and severity of loss from exposure to the threat. The assessment step is the application of quantitative or qualitative measures to determine the level of risk associated with a specific threat. This process defines the probability and severity of an undesirable event that could result from the threat.



Risk Management

Risk Management is process used to identify, analyze, and mitigate the risk (comprised of threats, vulnerabilities, safeguards and assets), and provide strategies for sustaining the security requirements of an information asset.

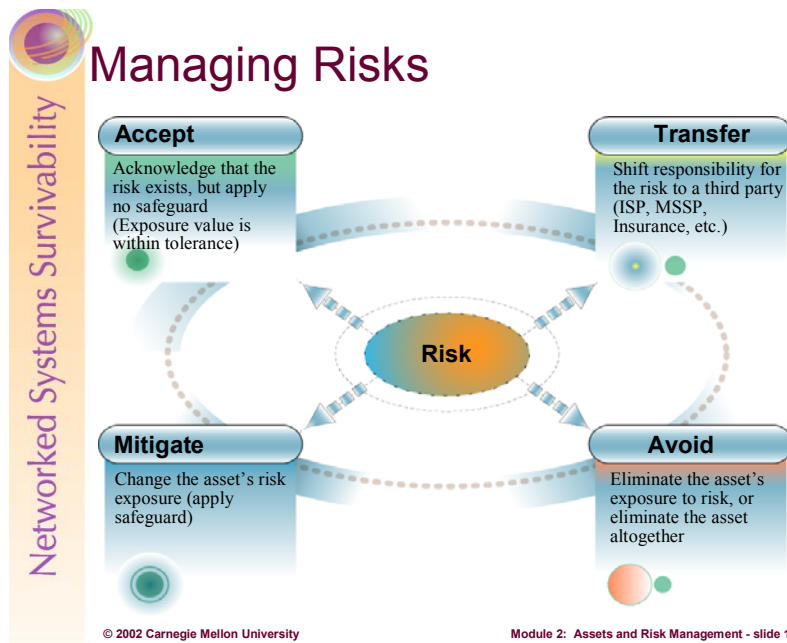


© 2002 Carnegie Mellon University

Module 2: Assets and Risk Management - slide 17

Risk Management

Risk management should be a well defined and established process. Effective risk management can save resources, reduce mishaps, and even save lives.



Organizations have four options when deciding how to manage risks:

Accept

If an organization chooses to accept risk, it does so with full knowledge of the potential threats and vulnerabilities to the asset. It may be that the asset's exposure is acceptable or within some level tolerance. For example, an organization recognizes the threat that usernames and passwords could be compromised by administering systems remotely with telnet, a pass-in-the-clear protocol. However, the organization decides that the risk is not great enough to warrant a safeguard (i.e., encrypted sessions with SSH or IPsec).

Mitigate

Mitigating risk is actively applying safeguards to reduce the asset's level of exposure. In the above telnet example, the organization could mitigate the risk by (a) denying all management traffic to the remote systems that is not encrypted and authenticated, and (b) writing an organizational policy that acts as a deterrent (i.e., any attempt to compromise access controls on organizational systems will be met with stiff disciplinary action).

Transfer

Transferring risk occurs when an organization decides to contract with a third party to mitigate the risk. For example, an organization can transfer the risk of losing data (and support the goal of mission survivability) by contracting with a service provider who maintains an offsite data backup and recovery capability. Although risk transference does not change probability or severity of a threat, it may decrease the probability or severity of the organization's risk. At a minimum, the organization's risk is greatly decreased or eliminated because the possible losses or costs are shifted to another entity.

Avoid

Avoiding risk means that the organization eliminates the asset's exposure or even the asset itself. An example might be the replacement of historically vulnerable platforms (like Internet Information Server) with hardened platforms like a Bastille/Apache Web server solution.¹

¹ <http://www.bastille-linux.org/>

Networked Systems Survivability

Risk Transference Issues

- Outsourcing Risk
- Trust dilemma
- Residual risk

The illustration depicts two men in a business setting. One man is seated at a desk, and the other is standing, holding a document labeled 'CONTRACT'. They are shaking hands. Two thought bubbles are shown: one above the seated man shows a dog biting a person's arm, and another above the standing man shows a person being hit by a dog. The background is a simple office environment.

© 2002 Carnegie Mellon University Module 2: Assets and Risk Management - slide 19

Risk Transference Issues

Because you cannot mitigate, let alone identify, all risks, at some point you have to trust someone or something to take the appropriate action or to function as designed. For example, you may have to trust people, systems, programs, data, etc., to handle and operate on information in a manner that upholds its security requirements.

If an organization has transferred risk to another party such as a managed security service provider (MSSP), the risk has not been completely removed. The client organization must trust in the effectiveness of the MSSP. As a result, there is still a residual risk that the MSSP may not be able to meet the expectations of the client all of the time. The responsibility (and consequences) of transferred risks are still retained by the organization.

Historically, programming and computer science have been taught in an environment that assumes that trust exists. As a result, many systems and software currently deployed are not designed to sufficiently guard against information survivability problems.

Beyond placing blind trust in the individuals and technology that protects information assets, you can apply monitoring to the risk you have accepted as well as the risk that you currently mitigate. In fact, monitoring accepted or transferred risks works in the same fashion as monitoring known, mitigated risks. For monitoring to be effective, risks that are managed or accepted must again be documented and understood by the organization and its employees.

Review Questions



1. What are the components of risk?
2. Why do we prioritize one asset over another?
3. What two properties are analyzed and calculated as part of a simple risk assessment?
4. What are a few of the items completed in a risk assessment?

© 2002 Carnegie Mellon University

Module 2: Assets and Risk Management - slide 20

1. What are the components of risk?

Risk is composed of *assets* (something of value to the organization), *threats* (threat actors, known and unknown vulnerabilities, potential attacks), *outcomes* (disclosure, modification, destruction/loss, interruption), and the probable *loss or impact* (damage done to reputation, confidence, finance, legal, performance, etc.).

2. Why do we prioritize one asset over another?

We prioritize assets so that the limited resources (funding, system/security administrator time, technology, support), can be applied efficiently to protect those assets. We must perform this type of activity to gauge what assets could cause an adverse impact to the organization upon failure (e.g., disclosure, modification, destruction, or interruption).

3. What two properties are analyzed and calculated as part of a simple risk assessment?

Probability and severity

4. What are a few of the items completed in a risk assessment?

1. Identifying critical information assets as they align with an organization's mission
2. Validating threats to the critical assets and areas of concern
3. Determining security requirements of the critical assets, as defined by the organization
4. Identifying current protection strategies and mechanisms supporting the assets
5. Identifying organizational vulnerabilities arising from gaps in the fundamental as well as security practices of the organization
6. Identifying key infrastructure components that support the processing, storage, and transmission of the critical assets
7. Identifying technological vulnerabilities and current deficiencies that exist on key components of the infrastructure
8. Analyzing current risks to critical assets due to the above
9. Recognizing required and necessary protection strategy changes and development
10. Specifying mitigation plans and action items to protect the critical assets



Module Summary

- Assets and asset value must be understood
- Risk can be both qualitative and quantitative
- Risk management
- Risk can be mitigated, but never eliminated

© 2002 Carnegie Mellon University

Module 2: Assets and Risk Management - slide 21

Sustaining and improving information security is a continuous risk management activity. Risk is comprised of assets (something of value to the organization), threats (concerns related to undesirable outcomes), safeguards, and vulnerabilities (weaknesses creating the possibility for threats to negatively impact the organization).

Risk analysis, a major component of risk assessment, helps to identify the possibility of certain risks and the impact when risk is realized to an information asset. Because information cannot be realistically managed to have no risk, at some point risk must be accepted.

Bibliography (Sources used throughout):

Alberts, C. Dorofee, A. "OCTAVE Method Implementation Guide Version 2.0." June 2001. Software Engineering Institute, Carnegie Mellon University.

Summers, R. Secure Computing: Threats and Safeguards. McGraw-Hill, 1997.

Various organizational practices and developing methodologies derived from work in the Survivable Enterprise Management Team within the Networked Systems Survivability (NSS) Program, Software Engineering Institute, Carnegie Mellon University.

[Allen 2002] Julia H. Allen, Carol A. Sledge. Shifts in thinning...

[Krutz 2001] Ronald L. Krutz, Russell Dean Vines. The CISSP Prep Guide...

The Naval Safety Center. <http://www.safetycenter.navy.mil/orm/default.htm>