Unisys Security Solutions

The Challenges of Todays Enterprise

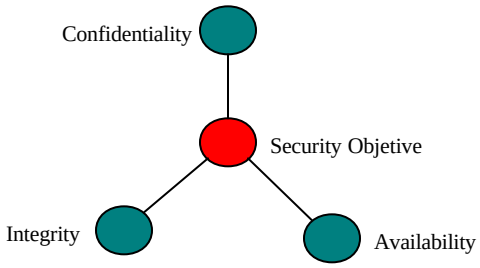
Ricardo Villadiego
ricardo.villadiego@unisys.com
Regional Sales Manager
Unisys Security Solution
Latin America and Caribbean Group

Unisys

What's Security?

What are we trying to accomplish again?

- The crux of security is to protect the company's assets.
- Security is based on the CIA triad :



Unisys

The crux of security and every security program is to protect the company's asset. In this sense, Risk managemenet will identify the assets, discover the risk that threaten them and estimate the potential damage and loss a company can endure if any of this risk become real.

The main three principles around the security concepts are confidentiality, integrity and availability these are reffered to as the CIA triad, the level of security required to accomplish these principles differs per company because their security goals and requirements may be differents.

Confidentiality: Provides the ability to ensure that the neccesary level of secrecy is enforced at each junction of data processing and prevention of unauthorized disclosure.

Integrity: is uphelp when the assurance of accuracy and reliability of information and system is provided, and unauthorized modification of data is prevented

Availability: Ensures the reliability and timely access to data and resources to authorized individuals.

Many times the words “threat”, “vulnerability”, “exposure”, and “risk” are used to represent the same thing even though they have different meanings and relationship to each other. It’s important to understand each word’s definition, but more importantly you should understand their association to each other.

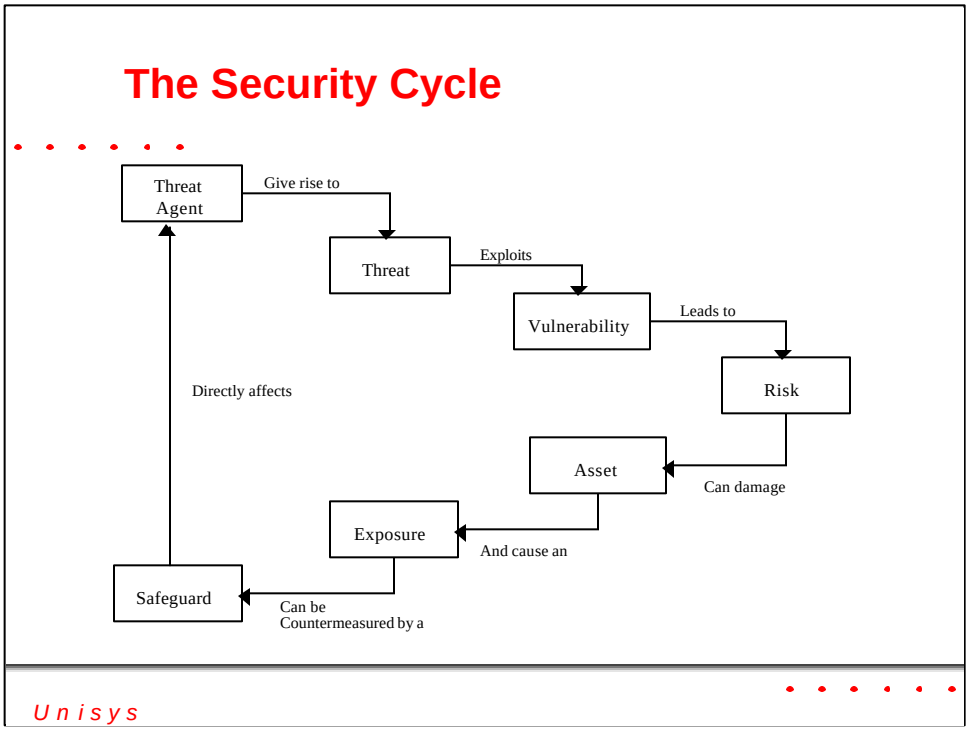
A ***vulnerability*** is a software, hardware, or procedural weakness that may provide an attacker the open door he is looking for to enter a computer or network and have unauthorized access to resources within the environment.

A ***threat*** is any potential danger to information or system, a Threat Agent could be an intruder accessing the network throught a port on the firewall , a process accesing data in a way that violates the security policy.

A ***risk*** is the likelihood of a threat agent taking advantage of a vulnerability. A risk is the loss potential, or probability, that a threat will exploit a vulnerability. If a firewall has several ports open, there is a higher risk that an intruder will use one to access the network in a unauthorized method.

An ***exposure*** is an instance of being exposed to lossess from a threat agent. A vulnerability can caused an organization to be exposed to possible damages

A ***countermeasure***, or safeguard, mitigates the potential risk. A countermeasure is a software configuration, hardware, or procedure that eliminates a vulnerability or reduce the risk of a threat agent from being able to exploit a vulnerability. Counter measures can be strong password management, a security guard, etc.



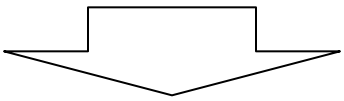
The cycle in the slide could be what happen in every company with the virus problem, for instance:

If a company has antivirus software only on the servers and the virus signatures are not kept up to date, this is a vulnerability. The company is vulnerable to virus attacks.The threat is a virus showing up in the environment and disrupting productivity. The likelihood of a virus showing up in the environment and causing damage is the risk.

Because there is a possibility of losing or corrupting data from a virus attack, the company now has an exposure. The countermeasures in this situation are to update the signatures and install the antivirus software on all computers.

Security Management

- Risk Management : To identify the assets, discover the risk that threaten them and …
- Security Policies: Provide directions for the security activities …
- Security Education: To take the security policies to every employee …



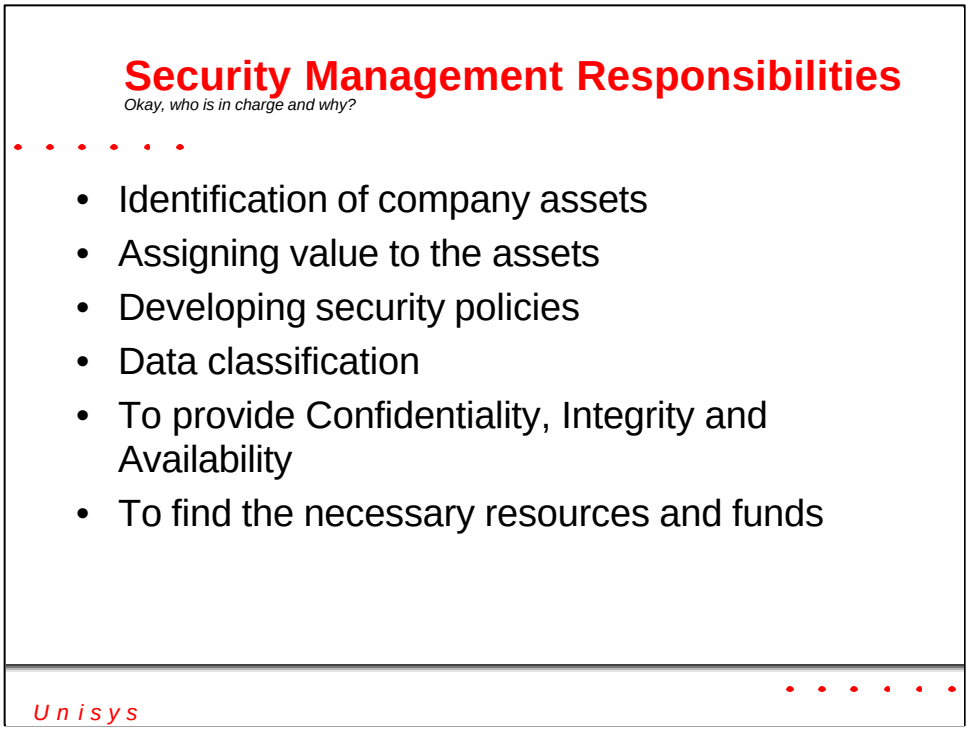
Corporate Security Program

Unisys

The concept security management includes risk management, security policies, and security education. These three core componets serve as the foundation of a corporation's security program. An again, the crux for security and a security program is to protect the company's assets.

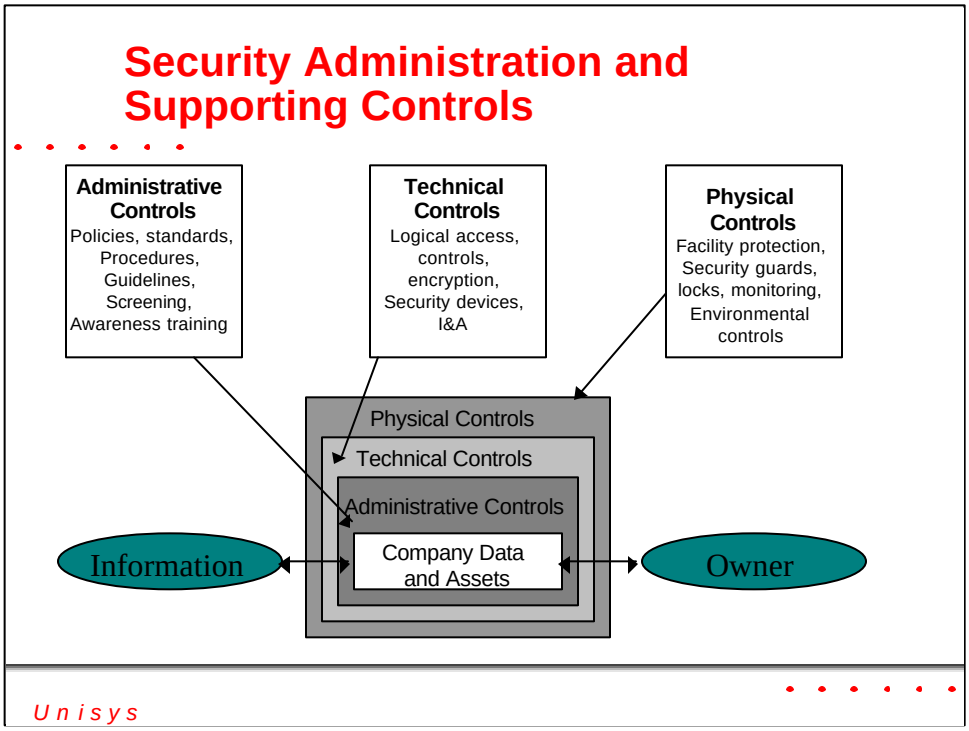
Risk management will identify these assets, discover the risk that threaten them, and estimate the possible damage and loss a company could endure if any of this risk become real. The result of the risk analysis help management to develop applicable ***security policies*** that provide security direction for the security activities that will take place in the company and express the value that management places on the company's security program.

Security education takes this information to each and every employee within the company so that everyone is properly informed and can more easily works towards the same security goals.



Security management relies on the proper identification of a company's information assets, assigning values to these assets, developing , documenting, and implementing security policies, procedures, standards, and guidelines, which provides integrity, confidentiality and availability.

Many companies only look at the business and productivity elements of an equation and figure that information and computer security fall within the IT administrator's responsibilities. In these situation, management is not taking computer and information security seriously and it will most likely remain underdeveloped, unsupported , and unsuccessful. Security needs to be addresses at the highest level of management.



The ***information owner*** is usually a senior executive within the management group of the company. The information owner has the final corporate resposibility of data protection and would be the one held liable for any negligence when it comes to protecting the company's information assets. The person who hold this role is responsible for assigning a classification to the information and dictating how the information should be protected.

Information owner should dictate who can access resources and how much capacity users can possess pertaining to those resources. The security administration's job is to make sure this happens. Administrative, technical and physical controls should be implemented to achieve this management directives.

Administrative controls include the development and publication of policies, standards, procedures, and guidelines, the screeining of personnel, security awareness training, the monitoring of system activities, and change control procedures.

Technical controls consist of logical access control mechanisms, password and resource management , identification and authentication methods, security devices, and configuration of the network

Physical controls entail controlling individual access into the facility and different departments, locking systems and removing unnecessary floppy or CD-ROM drives, protecting the perimeter of the facility and so on.

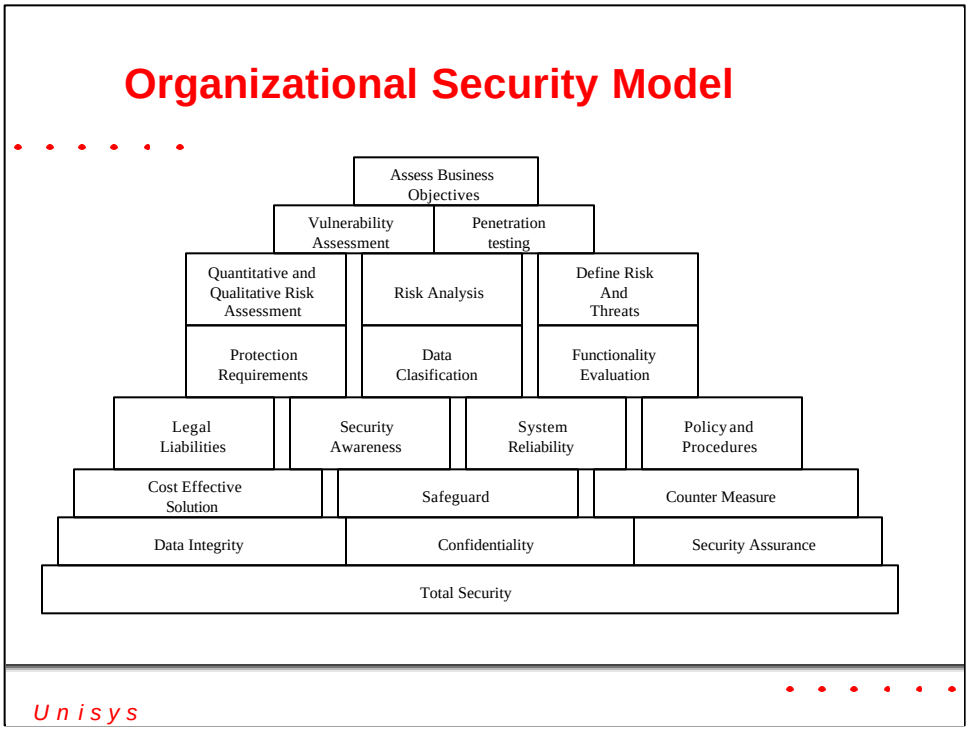
The Top-Down Aproach for Security

- When designing a security program the end result expected need to be determined and realized.
- The Security Policy works as a blueprint for a company's security program
- A top-down aproach mean that the initiation of a security program comes from the top management.

Unisys

When designing and/or implementing a security program, the functionality and end result expected need to be determined and realized. Many times companies just start locking down computers and installing firewalls without taking the time to understand the overall security requirements, goals, and assurance levels they expect from security as a whole within their environment. This process start from the top with very broad ideas and terms (blueprint) and works its way down to detailed configuration setting and system parameters (windows and carpets). At each step, the overall security goals need to be kept in mind so that each added piece is sure to add more granularity to the intended goal and not splinter the main objectives by running in 15 different directions at once.

The security policy works as a blueprint for a company's security program and provides the necessary foundation to build upon. This policy needs to be taken seriously from the beginning and developed with the idea that it will continually be referenced to ensure that all security componets stay in step and work to accomplish the same objectives. The next step is to develop and implement procedures, standards, and guidelines that support the security policy and identify the security componets and methods that need to be put in place.

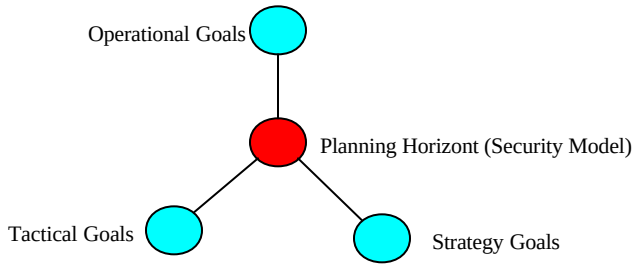


An organizational model is a framework made up of many entities, protection mechanism, logical and physical components, procedures, and configuration that all work together in a synergistic way to provide a security level for an environment. Each model is different, but all models work in layers: one layer providing support for the layer above it and protection for the layer below it.

The goal of a security model is assurance, which is the sum total of all security components an evironment that provide a level of confidence. Because a security model is a framework , companies are free to plug in different types of technologies, methods, and procedures to accomplish the neccesary security assurance level in their environment

Organizational Security Model

- A security model has different layers, but it also have different type of goals to accomplish in different times frames

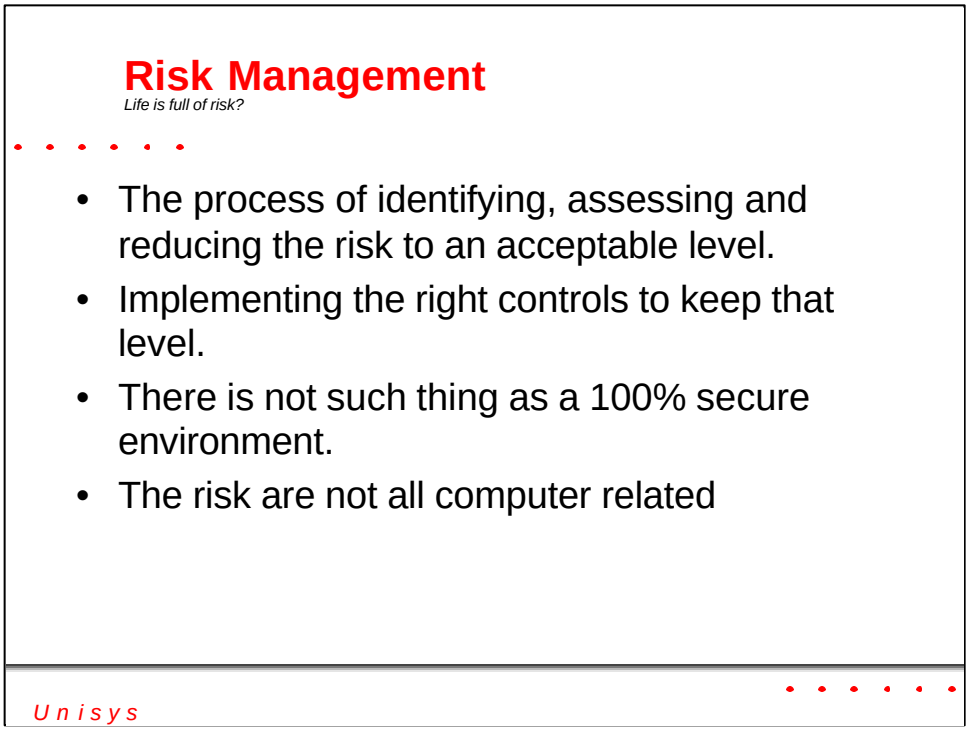


Unisys

A security model has different layers, but it also has different type of goals to accomplish in different time frames. There are daily goals or ***operational goals*** focus on productivity and task oriented activities to ensure that the company's functionality , mid-term goals or ***tactical goals*** that could be to integrate all workstation in one domain so more central control can be achieved and long-term goals or ***strategic goals*** that may involve moving all the branches from dedicated communications lines to site to site VPN and client to site VPN for all remote users instead of dial up entry.

This aproach to planning is called the ***planning horizon*** . A company cannot usually implements all changes at once, and some changes are larger than others. Many times certain changes cannot happens until other changes take place.

Security work best if it's operational, tactical, and strategic goals are defined and work to support each other, which can be much harder than it sound.



Risk is the possibility of something damaging happening; ***risk management*** is the process of identifying, assessing, and reducing this risk to an acceptable level and implementing the right mechanisms to maintain that level of risk.

There is not such thing as a 100% secure environment. Every environment has vulnerabilities and risk to certain degrees. The real skill comes in identifying these risk, assessing the probability of them actually ocurring and the damage they could cause, and then taking the right steps to reduce the overall level of risk in the environment.

Information Security Risks

- Physical Damage: Fire, water, power loss, vandalism
- Human Error: Accidental or intentional action
- Equipment malfunction: Failure of system
- Inside and outside attacks: Hacking , cracking
- Misuse of data:Sharing trade secrets
- Loss od data: Intentional or unintentional loss
- Application error: Computation errors, input errors

Unisys

When we look at information security, there are several types of risk a corporation needs to be aware of and address properly. The following items touch on the major categories

•Physical Damage: Fire, water, power loss, vandalism

•Human Error: Accidental or intentional action

•Equipment malfunction: Failure of system

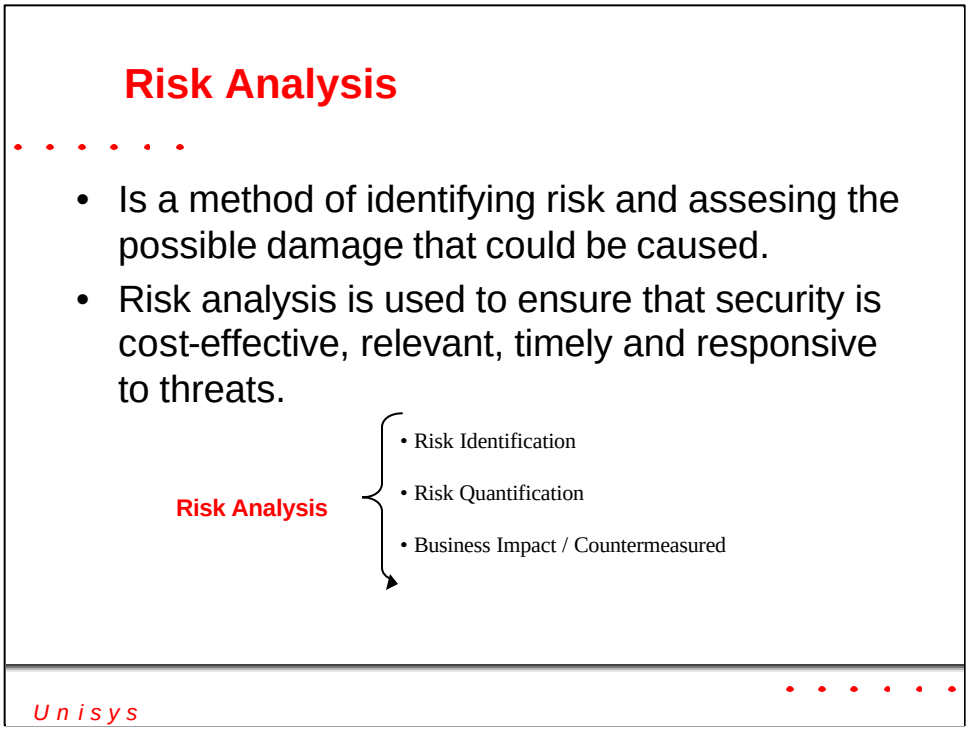
•Inside and outside attacks: Hacking , cracking

•Misuse of data:Sharing trade secrets

•Loss od data: Intentional or unintentional loss

•Application error: Computation errors, input errors

The threats need to be indentified, classified by category, and the actual magnitude of potential loss needs to be calculated. Real risk is hard to measure, but making priorities of the potential risks is attainable.



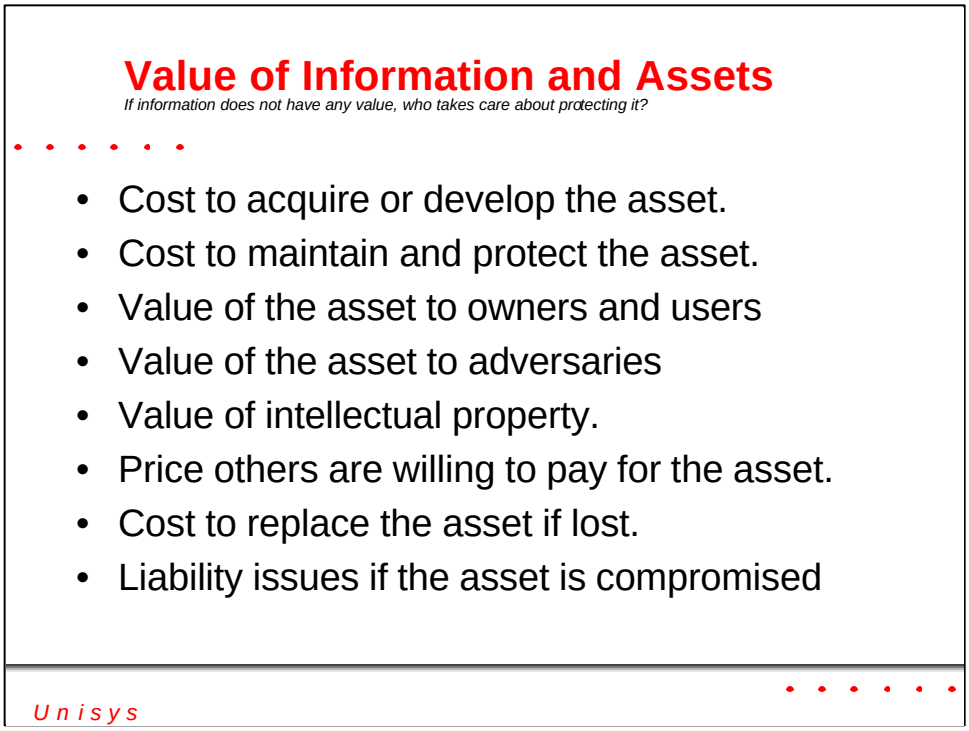
Risk analysis is a method of identifying risk and assessing the possible damage that could ba cause in order to justify security safeguard. A risk is the probability of a threat agent exploiting a vulnerability and creating damage to a system or environment. Risk analysis is used to ensure that security is cost-effective, relevant, timely, and responsive to threats.

Security can be quite complex, even for the well-versed security professionals, and it's easy to apply too much security, not enough security, the wrong security, the wrong security components, and spend too much money in the process withouth attainning the necessary objectives.

Risk analysis helps companies to prioritize their risk and shows them the amount of money that could be applied to protecting agains those risk in a sensible manner.

A risk analysis has three main goals: identify risks, quantify the impact of potential threats, and provide an economic balance between the impact of the risk and the cost of the countermeasure.

A risk analysis helps integrate the security program objectives with the company's business objective and requirements. The more the business and security objectives are in alignment, the more successful the two will be . The analysis also helps the company to draft a proper budget for a security program and the security components that make up the program.

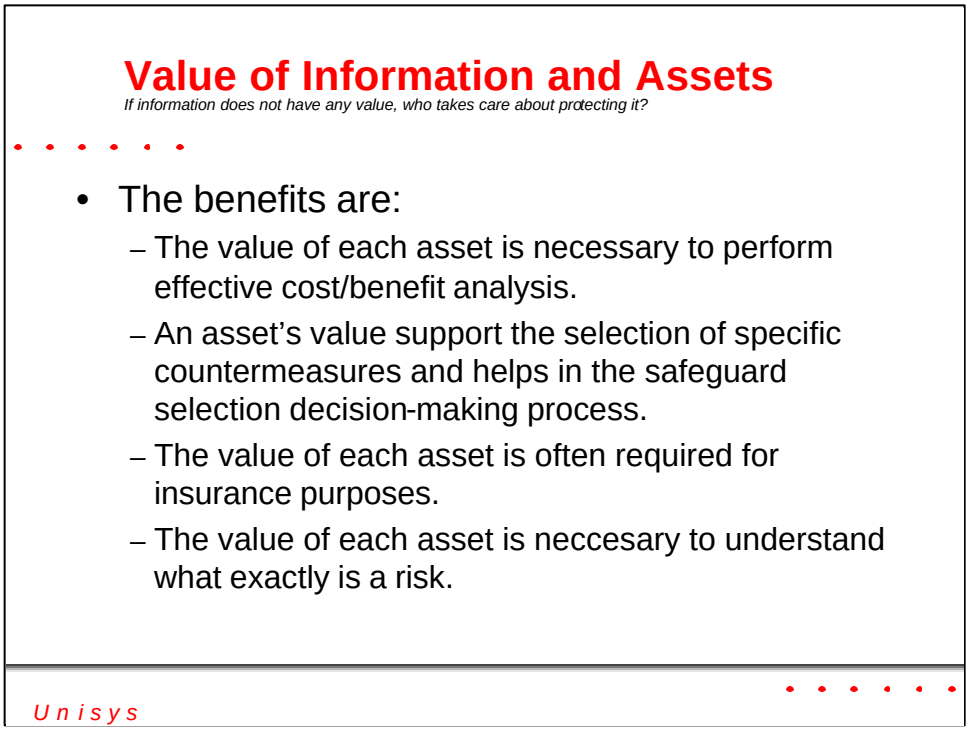


Information can have a quantitative and qualitative measure assigned to it, but this measurement needs to be derived. The actual cost of data is determined by the cost it takes to acquire, develop, and maintain it. The value is determined by the value it has to the owners, authorized, and unauthorized users. Some information is important enough for the company to go through the steps of making it a trade secret or the company may choose to copyright specific logos and trademarks.

The following issues should be considered when assigning value to information and assets:

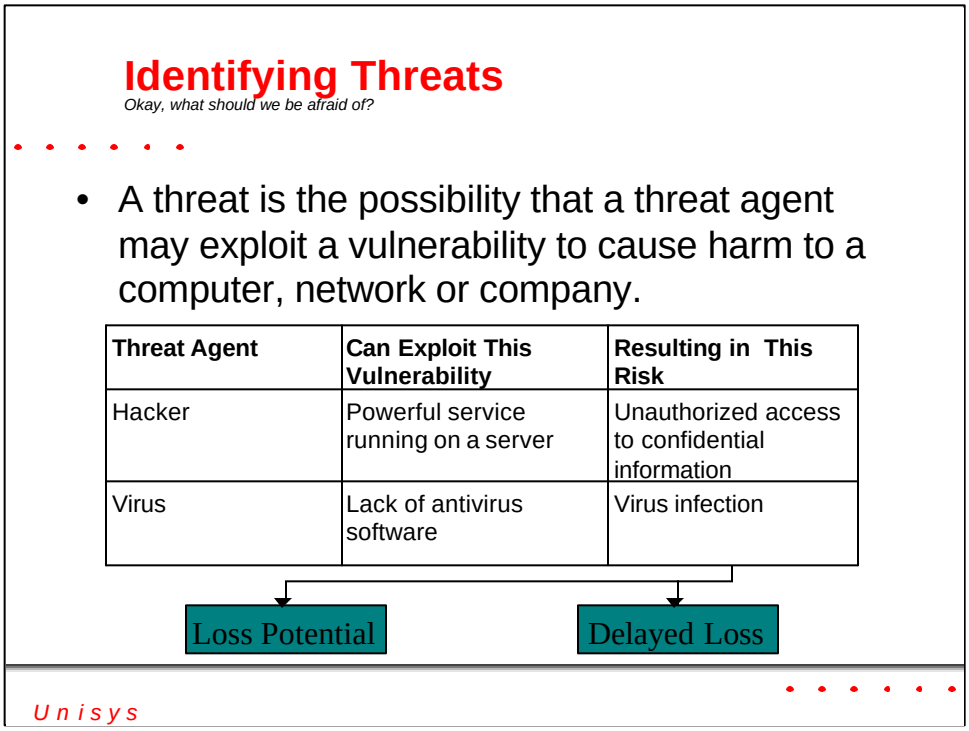
- Cost to acquire or develop the asset.
- Cost to maintain and protect the asset.
- Value of the asset to owners and users
- Value of the asset to adversaries
- Value of intellectual property.
- Price others are willing to pay for the asset.
- Cost to replace the asset if lost.
- Liability issues if the asset is compromised

Understanding the value of information is the first step to understanding what security mechanisms should be put in place and what funds should go towards this protection.



Determining the value of an asset can fulfill several different types of requirements a company may be facing, including the following:

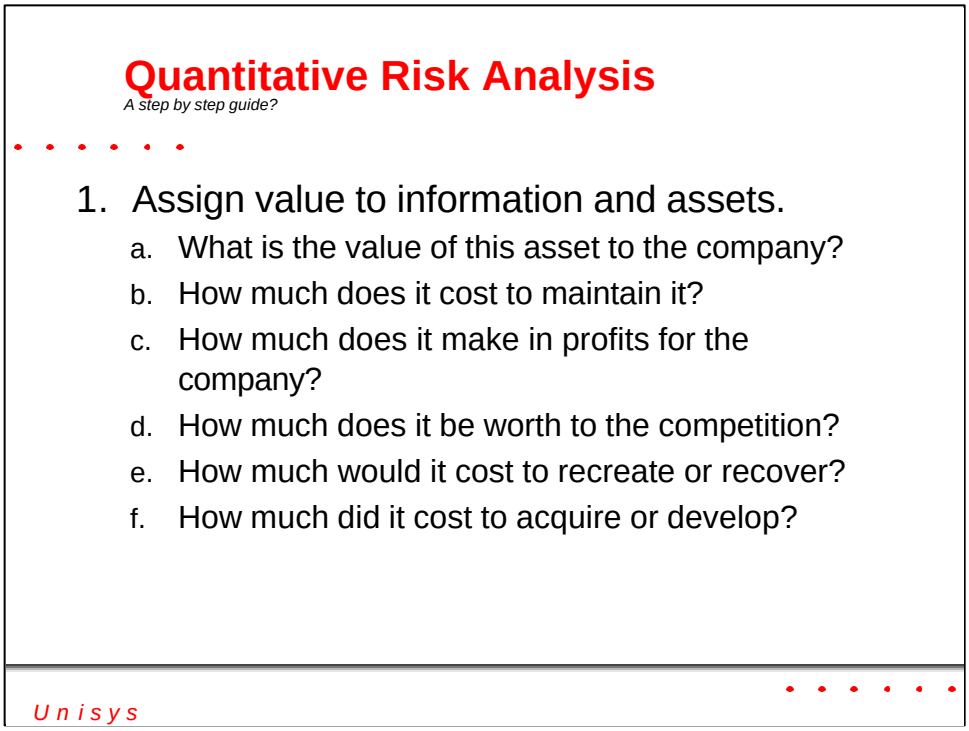
- The value of each asset is necessary to perform effective cost/benefit analysis.
- An asset's value support the selection of specific countermeasures and helps in the safeguard selection decision-making process.
- The value of each asset is often required for insurance purposes.
- The value of each asset is neccesary to understand what exactly is a risk.



Early it was stated that the definition of a threat is the possibility that a threat agent may exploit a vulnerability to cause harm to a computer, network or company. There are many types of threat agents that can take advantage of several types of vulnerabilities that can result in risks.

Risk have ***loss potential ,*** meaning that the company would lose something if a threat agent actually exploits a vulnerability. The loss can be corrupted data, destruction to system, unauthorized disclosure of confidential information, and a reduction of employee productivity. When performing a risk analysis, the team also needs to look at ***delayed loss*** when assesing the damage that can occur from a risk.

Delayed loss have negative effects on a company after a risk is initially exploited. The time period can be 15 minutes after the exploitation to years. Delayed loss issues can be reduced productivity over a period of time, reduce income to the company, and delayed collection of funds from the customers.



There are two types of aproach to risk analysis: ***quantitative*** and ***qualitative*** . Quantitative attempts to assign real numbers to the cost of countermeasures and the amount of damage that can take place . Qualitative also provide a concrete probability percentages when determining the likelihood of threats and risks.

Purely quantitative risk analysis is not possible because the method is attempting to quantify qualitative items

There are many methods and equation that could be used when performing a quantitative risk analysis and many different variables that can be inserted into the process. We're going to go over the main steps that happen in every risk analysis and assessment.

Assign value to information and assets.

a. What is the value of this asset to the company?
b. How much does it cost to maintain it?
c. How much does it make in profits for the company?
d. How much does it be worth to the competition?
e. How much would it cost to recreate or recover?
f. How much did it cost to acquire or develop?

Quantitative Risk Analysis

A step by step guide?

2. Estimate potential loss per risk.
   a. What physical damage can take place and how much would that cost?
   b. How much productivity can be lost and how much would that cost?
   c. What is the value lost if confidential information is disclosed?
   d. What is the cost of recovering of a virus attack?
   e. What is the cost of recovering of a hacker attack?
   f. Calculate the single loss expectancy (SLE) for each risk and scenario

Unisys

2. Estimate potential loss per risk.
   a. What physical damage can take place and how much would that cost?
   b. How much productivity can be lost and how much would that cost?
   c. What is the value lost if confidential information is disclosed?
   d. What is the cost of recovering of a virus attack?
   e. What is the cost of recovering of a hacker attack?
   f. Calculate the single loss expectancy (SLE) for each risk and scenario

Quantitative Risk Analysis

A step by step guide?

3. Perform a threat analysis.
   a. Gather information about the likelihood of each risk taken place.
   b. Calculate the probability of occurrence of each risk identified.
   c. Calculate the annualized rate of occurrence, which is how many times each risk could happen in a year (ARO)

Unisys

3. Perform a threat analysis.
   a. Gather information about the likelihood of each risk taken place.
   b. Calculate the probability of occurrence of each risk identified.
   c. Calculate the annualized rate of occurrence, which is how many times each risk could happen in a year (ARO)

Quantitative Risk Analysis

A step by step guide?

4. Derive the overall loss potential per risk
   a. Combine potential loss per risk.
   b. Calculate the annualized loss expectancy (ALE) per risk by using the information calculated in the first three steps.
5. Choose remedial measures to counteract each risk.

Unisys

4. Derive the overall loss potential per risk
   a. Combine potential loss per risk.
   b. Calculate the annualized loss expectancy (ALE) per risk by using the information calculated in the first three steps.
5. Choose remedial measures to counteract each risk.

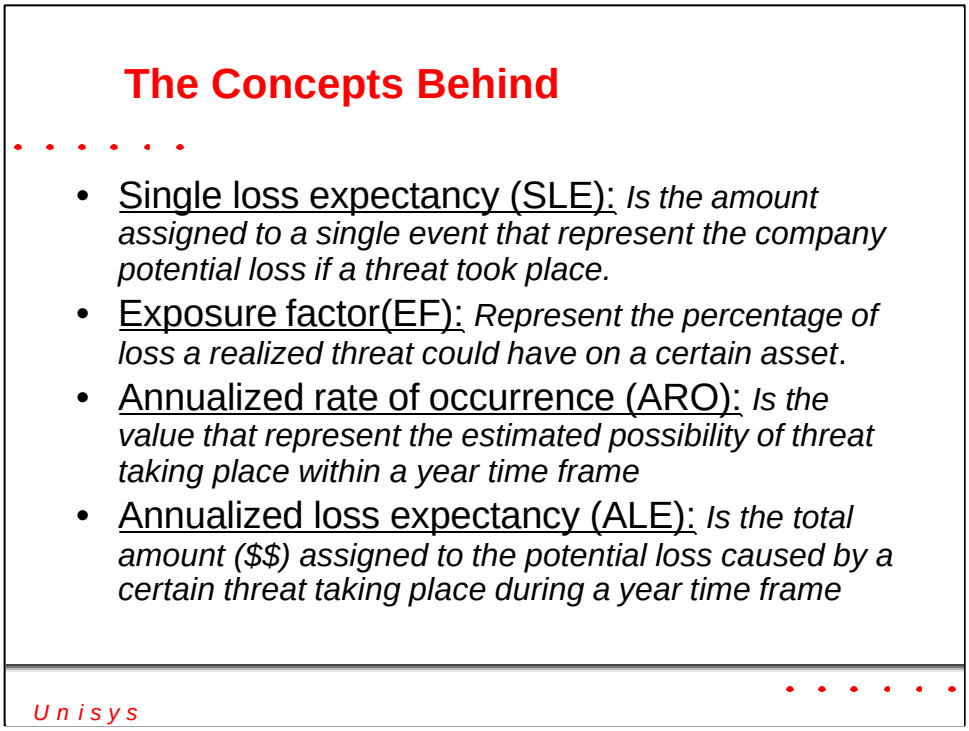
Quantitative Risk Analysis

A step by step guide?

6. Reduce, assign, or accept the risk.
    a. Risk reduction methods.
        i. Install security controls
        ii. Improve procedures
        iii. Contingency plan
    b. Risk assignement.
        a. Buy insurance to transfer some or all of the risk
    c. Risk acceptance.
        a. Live with the risk and spend no money towards protection

Unisys

6. Reduce, assign, or accept the risk.
    a. Risk reduction methods.
        i. Install security controls
        ii. Improve procedures
        iii. Contingency plan
    b. Risk assignement.
        a. Buy insurance to transfer some or all of the risk
    c. Risk acceptance.
        a. Live with the risk and spend no money towards protection



Because we are stepping through a quantitative risk analysis, real numbers are used and calculations are necessary:

Single loss expectancy (SLE): Is the amount ($$) assigned to a single event that represent the company potential loss if a threat took place.

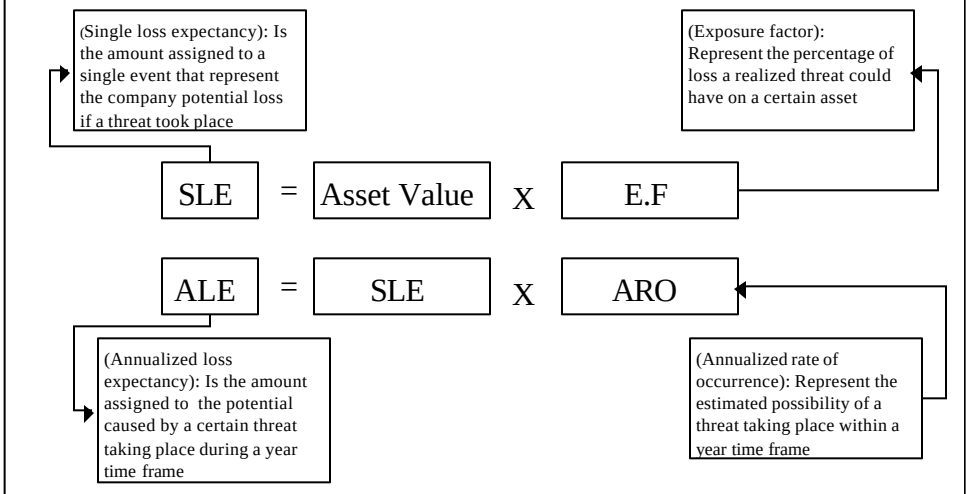
Exposure factor(EF): Represent the percentage of loss a realized threat could have on a certain asset.

Annualized rate of occurrence (ARO): Is the value that represent the estimated possibility of threat taking place within a year time frame. The range can be from 0.0 (never) to 1.0 (always) and anywhere in between. For example if the probability of a hurrican taking place in Rio de Janeiro once in 1000 years the the ARO value is 0.001

Annualized loss expectancy (ALE): Is the total amount ($$) assigned to the potential loss caused by a certain threat taking place during a year time frame.

How do we calculate that?

ALE=1/Log(x^2) with x=e^(EF)



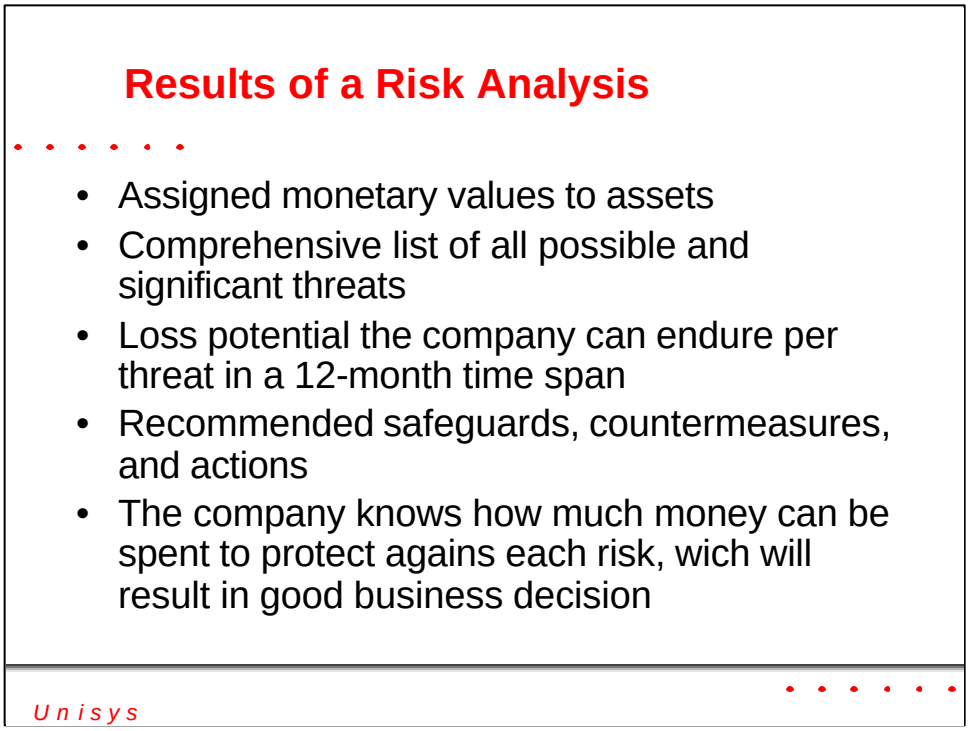
A Quick Example

Asset	Risk	Asset Value	EF	SLE	ARO	ALE
Facility	Fire	$560.000	0.412	$230.000	.25	$57.500
Trade Secret	Stolen	$43.500	0.920	$40.000	.75	$30.000
File Server	Failed	$11.500	1.000	$11.500	.5	$5.750
Data	Virus	$8.900	0.730	$6.500	.8	$5.200
Customer credit card info	Stolen	$323.500	0.927	$300.000	.65	$195.000

$293.450

Intelligent Decisions

Unisys



The risk analysis team should have clearly defined goals and results that they are seeking. The following gives a short list of what generally es expected from the results of a risk analysis.

•Assigned monetary values to assets

•Comprehensive list of all possible and significant threats

•Loss potential the company can endure per threat in a 12-month time span

•Recommended safeguards, countermeasures, and actions

•The company knows how much money can be spent to protect agains each risk, wich will result in good business decision

Although this list looks small, there is usually an incredible amount of detail under each bullet item.

After a risk analysis the compnay knows how much money can be spent to protect again each risk, wich will result in a good business decision instead of just buying protection here and there without a clear understanding of the big picture.

A Qualitative Aproach

- Does not assign numbers and monetary values to assets and losses
- Walk through different scenarios of risk possibilities and rank the seriousness of the threats and the sensitivity of the assets
- Qualitative techniques include judgement, intuition and experience
- Examples are Deplhi, brainstorming, focus groups, one-on-one meeting and inteviews.

Unisys

Another method of risk analysis is qualitative, which does not assign numbers and monetary values to components and losses. Instead, qualitatives methods walk through different scenarios or risk possibilities and rank the seriousness of the threats and the sensitive of the assets. Qualitative analysis techniques include judgement, intuition, and experience. Examples of qualitative techniques are Delphi, brainstorming, story-boarding, focus groups, surveys, questionnaries, checklist, one-one meeting and interviews.

A Qualitative Example

Threat= Hacker Accessing Confidential Information	Severity of Threat	Probability of threat taking place	Potential loss to the company	Effective-ness of a Firewall	Efective-ness of a IDS	Effective-ness of a Honey Pot
IT Manager	4	2	4	4	3	2
Database Administrator	4	4	4	3	4	1
Application Programmer	2	3	3	4	2	1
System Operator	3	4	3	4	2	1
Operational Manager	5	4	4	4	4	2
Results	3.6	3.4	3.6	3.8	3	1.4

Unisys

The team that is performing a risk analysis gather personnel who have experience and education on the risk being evaluated, When this group is presented with a scenario that describe a risk and loss potential, they will respond with their gut feeling on how the risk will actually carry out and what extend of damage may result.

Qualitative Vs Quantitative

Attribute	Quantitative	Qualitative
Requires more complex calculation	X	
Degree of guesswork that is involved		X
Is easily automated	X	
Provides a cost/benefit analysis	X	
Uses independent and objective metric	X	
Provides the opinions of the staff that knows the processes best		X
Shows clear-cut lossess that can be accrued within one year	X	

Unisys

Each method has its advantages and disavantages and the table above is a list of some of the differences between the two methods.

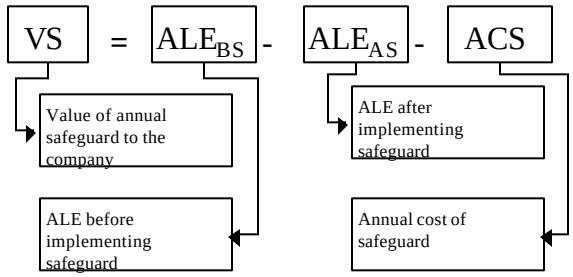
The risk analysis team, management , risk analysis tool, and culture of the company will dictate which approach, quantitative or qualitative will be used. Management may feel very confortable with their staff's opinion and just want the data gathered and presented.

The goal of either method is to estimate a company's real risk and rank the severity of the risk so the correct countermeasures can be put into place using a practical budget.

Countermeasure Selection

Okay, so we know we are at risk, we know the probability of it happening, now what we do?

- A countermeasure (safeguard) must make good business sense



Unisys

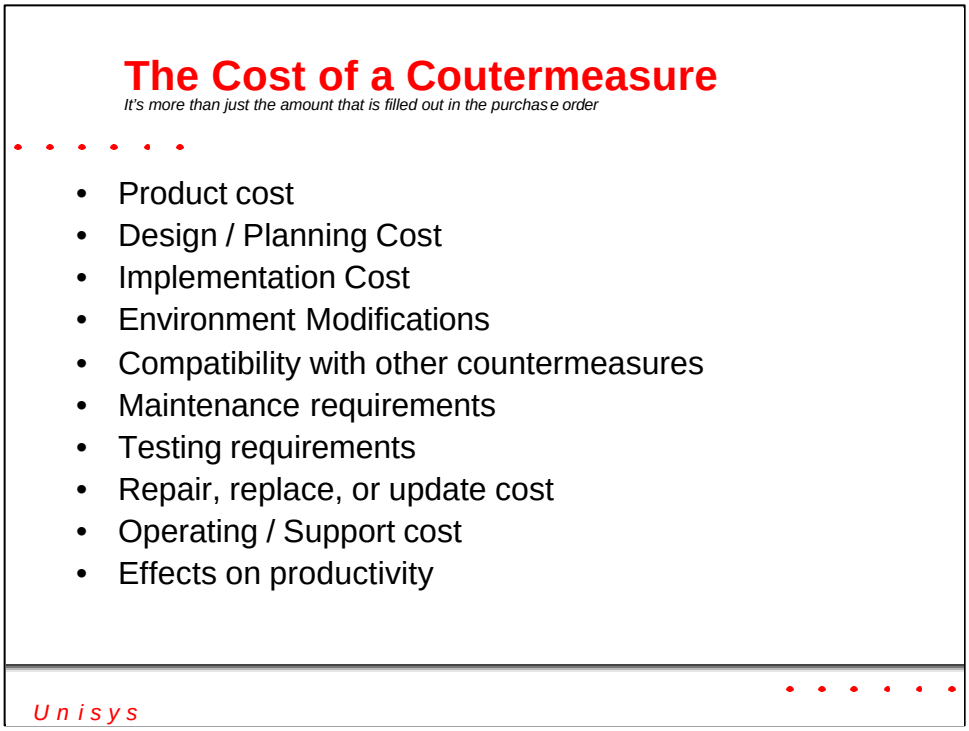
A countermeasures, sometimes called a safeguard , must make good business sense, Good business sense means that it is cost-effective and that its benefit outweighs or equals its cost. This requires another type of analysis: a ***cost/benefit analysis.***

A commonly used cost/benefit calculation for a given safeguard is:

(ALE before implementing safeguard) - (ALE after implementing safeguard) – (annual cost of safeguard) =

value of safeguard to the company

For example is the ALE of a the threat of a hacker bringing down a Web server is $12.000 and after the suggested safeguard is implemented the ALE is now $3.000 and the annual cost of maintenance and operation of the safeguard is $650 then the value of this safeguard is $8.350 each year.



The cost of a countermeasure is more than just the amount that is filled out on the purchase order. The following items need to be considered and evaluated when deriving the full cost of a safeguard.

- Design / Planning Cost
- Implementation Cost
- Environment Modifications
- Compatibility with other countermeasures
- Maintenance requirements
- Testing requirements
- Repair, replace, or update cost
- Operating / Support cost
- Effects on productivity

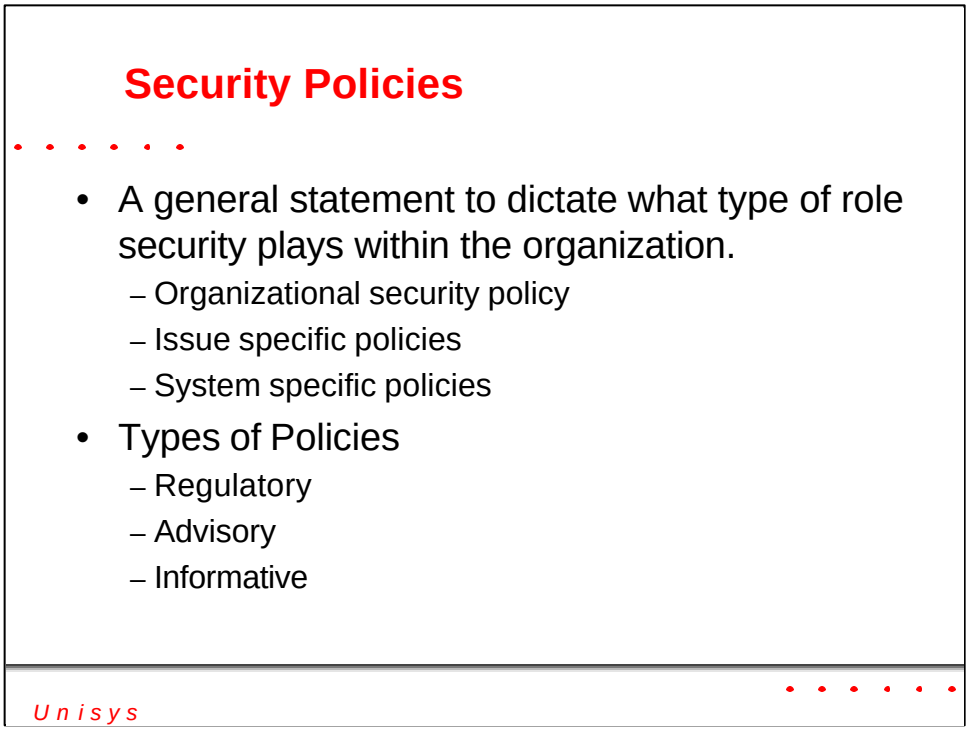
Handling the Risk

Now that we know the risk, what do we do with it?

- Transfering : To a insurance company
- Reduce : Implementing countermeasures
- Rejecting : Ignore the risk
- Accept : The company understand the risk and the cost of damage.

Unisys

Once a company knows the amount of total and residual risk they are faced with, they must decide how to handle it. There are four basic ways of dealing with risk: transfering, rejecting, reducing, or accepting the risk.



A security policy is a general statement produced by senior management to dictate what type of role security plays within the organization. A security policy can be an organizational policy, issue-specific policy or system-specific policy:

In an ***organizational security policy***, management establishes how a security program will be set up, establishes the program's goals, assign responsibilities, shows the strategic and tactical value of security, and outlines how enforcement should be carried out.

Issue-specific policies address specific security issues that management fells need more detailed explanation and attention to make sure a comprehensive structure is built and all employees understand how they are to comply to these security issues.

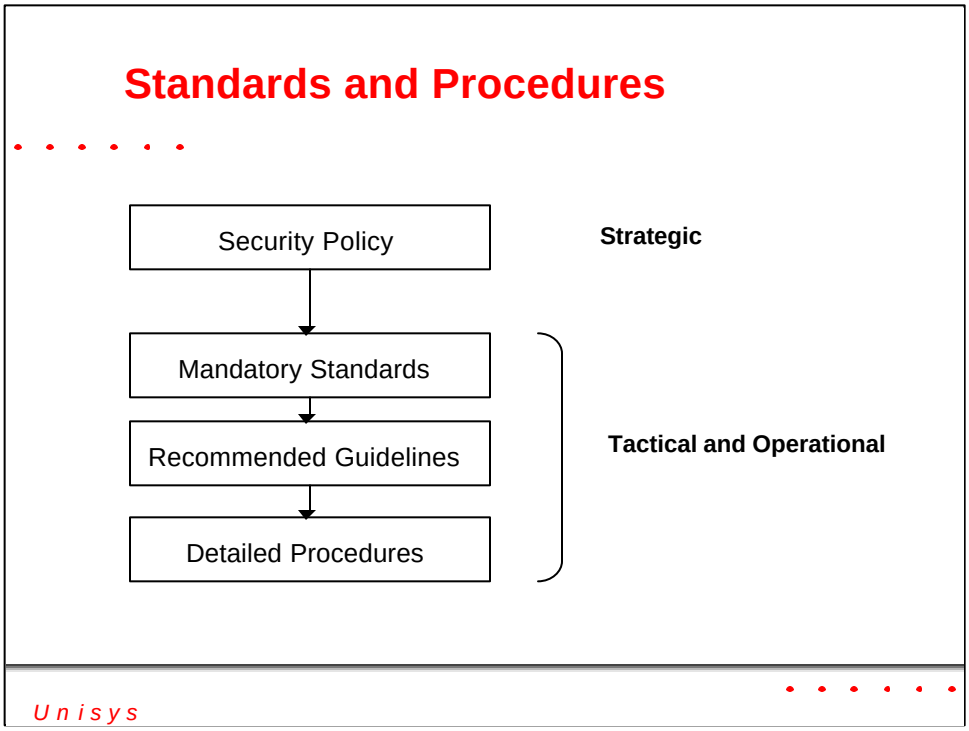
A ***System-specific policy*** present the management decision that are closer to the actual computers, networks, applications, and data. This type of policy can provide and approved software list, which contains a list of applications that can be installed on individuals workstation.

Policies also fall into one of the following categories:

Regulatory: This policy is written to ensure that the organization is following standars set by a sepecific industry and is regulated by law.

Advisory: This policy is written to strongly suggest certain types of behaviors and activities which should take place within the organization.

Informative: This policy is written to inform employees of certain topics. It's no an eforceable policy, but one to teach individuals about specific issues relevant to the company



Policies are written in broad and overview terms to cover many subjects in a general fashion. Much more granularity is needed to develop the ways and methods that need to happen to actually support the policyand this happens with the use of procedures, standards and guidelines.

Organization ***security standards*** specify how hardware and software products are to be used. They provide a means to ensure that specific technologies applications, parameters, and procedures are carried out in an uniformed way across the organization.

Baselines provide the minimun level of security necessary throughout the organization. A consistent baseline needs to be established before the security architecture can be propertly developed. Standards are usually developed from baseline and baseline are sometimes considered the abstraction of standards

Guidelines are recommendations actions and operational guides to users, IT staff, operation staff, and others when a specific standard does not apply. They deal with the methodologies of securing computers and their software.

Procedures are detailed step by step actions to achieve a certain task. The steps can apply to users, IT staff, operation staff, security members and others who may need to install or configure a computer component.

Resources For Security Policies and Procedures

- RFC2196 - The Site Security Procedures Handbook
  - obsoletes rfc1244 as of 9/97.
  - *http://ds.internic.net/rfc/rfc2196.txt*
- Some useful Web sites:
  - *http://www.gatech.edu/itis/policy/usage/contents.html*
  - *http://csrc.ncsl.nist.gov/secplcy/*

Unisys

It is difficult to find general resources for business oriented policies. Many companies consider their security policies to be sensitive information, however here are some links

Why Data Classification

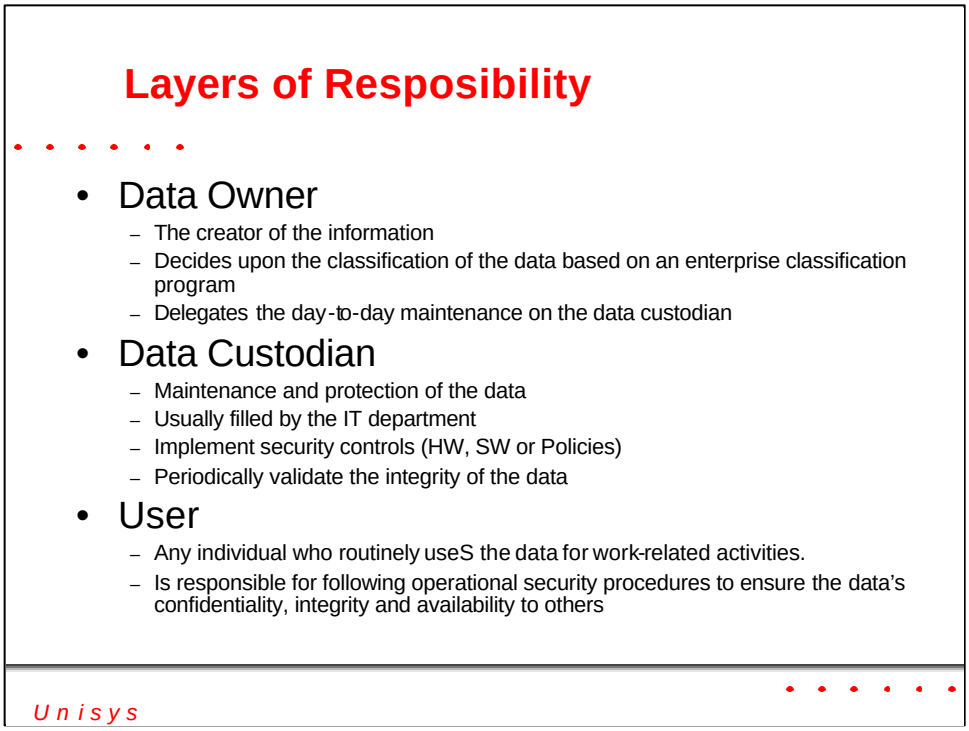
- To organize business information according to its value
- To Identify the level of the CIA triad required for each type of information
- To decide what security controls are needed for labeling, handling, transmission, storage, destruction
- Data classification help to ensure that the data is protected in the most cost-effective manner relative to its business value

Unisys

The relationale behind assigning assigning a value to data is to be able to gauge the amount of funds and resources that should go towards protecting it because not all data has the same value to the company. After the exercise to identifying important information it should then be properly calssified

Sample Data classification for non-military institutions

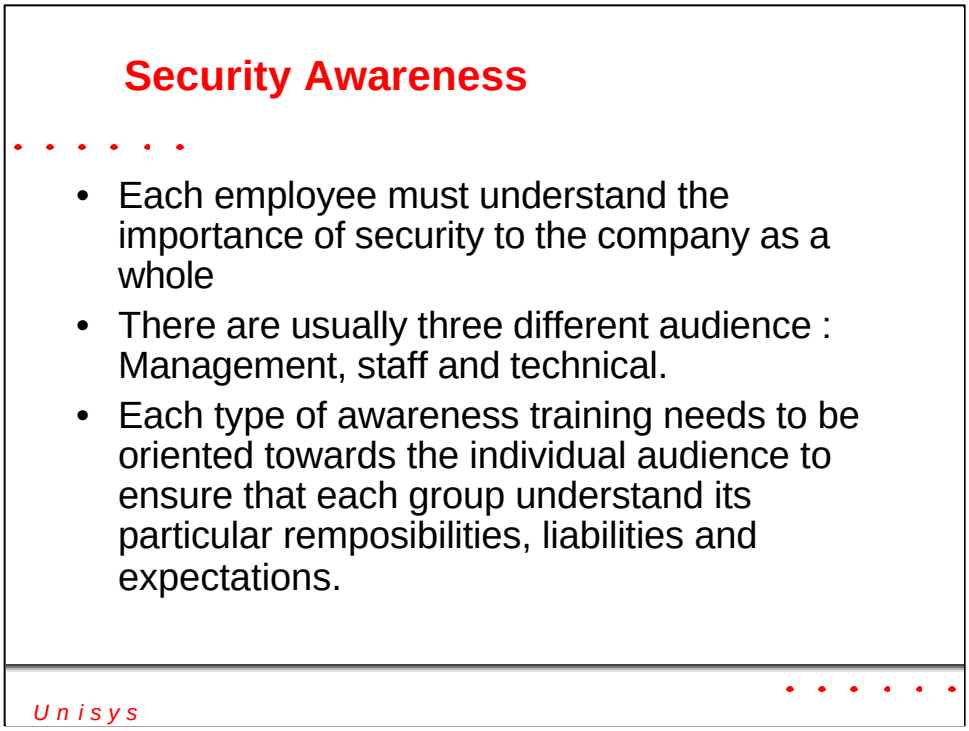
Classification	Definition
Confidential	- For use within the company only. - Data that is exempt from disclisure under the Freedom of information Act or other laws or regulation - Unauthorized disclosure could seriously affect a company
Private	- Personal information for use within a company - Unauthorized disclosure could seriously affect personnel
Sensitive	- Requires special precautions to ensure integrity of the data by protecting it from unauthorized modification or deletion - Requires higher than normal assurance of accuracy and completeness
Public	- All data does no fit into previous classes - Disclosure is not welcome but it would not cause an adverse impact to company or personnel.



The ***data owner*** is usually a member of senior management and is ultimately responsible for the protection and use of data. The data owner decides upon the classification of the data he is responsible for and alter this classification is the business needs arise. The data owner will delegate the resposibility of the day to day maintenance of the data, which is the responsibility of the data custodian.

The ***data custodian*** is given the responsibility of the maintenance and protection of the data. This tole is usually filled by the It department, usually by the network administrator, and the duties include performing backups of the data, implemeting security mechanism, periodically validating the integrity of the data, and so on.

The ***user*** is considered any individuals who routinely uses the data for work-related tasks. The user must have the necessary level of access to the datato perform the duties within her position and is responsible for following operational security procedures to ensure the data's confidentiality, integrity, and availability to others.



The management's directives pertaining to security is captured in the security policy, and the standards, procedures, and guidelines are developed to support these directives. However, this will not be effective if no one knows about these itemsand how the company expects them to be implemented.

For an organization to achieve the desired result of their security program, they must communicate the what, how, and why of security to their employees. It should be comprehensive, tailored for specific groups, and organization-wide. The goal is that each employee understand the importance of securityto the ompany as a whole to each individual. Expected responsibilities and acceptable behavior need to be clarified, and noncomliance repercursion that could range from a warning to dismissal need to be explained before being invoked.

U n i s y s

www.unisys.com/security