Security Policies

We all should have some form of security policy, even at home. In an organization, however, it must be established to ensure that people use the organization's hardware and software correctly to minimize the risk of a security related inconvenience or disaster.

First, click on the image or link below to get an overview of what a security policy actually is.

http://coursecontent.ntc.edu/CIT/husband/pois/lp6/m21-securitypolicy.html

Besides knowing what a security policy is, you should also be familiar with the following security policy concerns:

1. Balancing trust and control
2. Designing a security policy
3. Types of security policies

BALANCING TRUST AND CONTROL

Because security affects people and productivity, there will always be a fine line between who you can trust and how much control is enforced.

Deciding on the level of trust may lead to security problems by trusting everyone all of the time or may lead to problems keeping employees by not trusting anyone at any time. There usually is a good in-between mode giving trust where and when it is needed.

The amount of control used to implement a security policy will affect people in different ways.

Click on the image or link below to view the attitudes different user groups have toward security controls.

http://coursecontent.ntc.edu/CIT/husband/pois/lp6/m22-attitudes.html

DESIGNING A SECURITY POLICY

In an organization there are rules. Rules that are put into place to help users do their job are called standards and guidelines; these don't necessarily have to be followed, but it is recommended to do so. Policies, on the other hand, are rules that must be followed.

Click on the image or link below to see what some of these policy rules are.

http://coursecontent.ntc.edu/CIT/husband/pois/lp6/m23-policydefinition.html

It is difficult to precisely define each and every situation that can occur in an organization and set a policy to enforce it. Therefore, a form of language used in many policies is "**due care**". Due care is the conduct that a reasonable man or woman will exercise in a particular situation.

"Employees will exercise due care in opening attachments received from unknown sources." A reasonable person should know that an attachment from an unknown source could contain a virus.

Most organizations follow a security policy cycle that is three-phase:

1. Performing a risk management study.
2. Creating a security policy based on the risk management study.
3. Reviewing the policy for compliance.

PERFORMING A RISK MANAGEMENT STUDY

A risk management study takes a systematic and structured approach to minimize the risks of potential loss as they relate to given threats. Risk management typically involves 5 sequential steps:

1. Asset identification.
2. Threat identification.
3. Vulnerability appraisal.
4. Risk assessment.
5. Risk mitigation.

Asset Identification

Identify the items that are worth protecting such as data, hardware, personnel, physical assets, and software and then document their attributes and value.

Threat Identification

Determine who or what the threats are to the assets that you identified.

Vulnerability Appraisal

Determine current security weaknesses and how they might expose the assets to threats.

Risk Assessment

Determine the cost of an attack and the likelihood that the vulnerability is a risk to the organization.

Risk Mitigation

Determine what to do about the risks – if anything.

CREATE THE POLICY

Using the information gathered from the risk management study, a security policy is written to clearly define the steps the organization will deploy to the assets.

REVIEW THE POLICY FOR COMPLIANCE

This phase may also reveal a need to reevaluate risk and modify the security policy should organizational assets and resources be changed.

The cycle is a never ending process.

TYPES OF SECURITY POLICIES

Seldom do you see one large security policy to cover all aspects of an organization. It is much easier to create and maintain security modules (or sub-policies).

Here are some examples:

1. **AUP: Acceptable Use Policy.**

Defines the actions users may perform wile accessing systems and networking equipment.

2. **Security-Related Human Resource Policy.**

Introduces a new employee to the information technology resources of an organization and what the employee's rights and privileges are regarding those resources. This policy may contain language regarding penalties for violating policies.

3. **Personally Identifiable Information (PII) Policy.**

Outlines how the organization uses personal information it collects.

4. **Disposal and Destruction Policy.**

This policy addresses the disposal of resources that are considered confidential. This covers recycled computers, hard drives and written documents, for example. This policy may also address how long records are to be kept on file.

5. **Ethics Policy.**

Generally speaking, if a person has good moral values and makes decisions that are considered good and right by people, then they are ethical. If an organization, through ethics policies, help to craft ethical employees, the good, ethical practices of employees will make for a well-respected company. It is for this reason that having a good "code of ethics" is good practice.