

# **IDRBT's Working Paper No. 7**

## **Framework of IT Security Policy**

- *Ashutosh Saxena and V. P. Gulati*

### **ABSTRACT**

*Information is an important asset, which like other business assets, is of immense value to an organization. Therefore, it needs to be suitably protected. Information security is achieved by framing a suitable set of policies and procedures. In this work, we present a Framework of IT Security Policy by suitably classifying the security policy into three levels. The first and foremost is the top-level security policy, which outlines a clear direction to the information security needs of an organization. The second is the security architectural policy, which is developed in accordance with the top-level security policy and consists of various components of the security profile. The third, security operational policy provides specific guidance on allocation of security roles, responsibility, do's and don'ts within the organization. We conclude with a criteria for evaluating a security policy and remarks on interpretation and publicizing the IT security policy and methodology to define the security policy.*

### **1.0 Introduction**

The world of computers has changed drastically, from the earlier mainframe/mini-computers/standalone PC and computer centers to the present day interconnected computers. In the earlier decades computers were kept in locked rooms and Information System staff made sure they were carefully managed and physically secured. Links outside the company-computing environment were unusual. Computer security threats were rare, and basically came from insiders; authorized users misusing accounts, theft and vandalism, and so forth. These threats were well understood and dealt with using standard techniques; computers behind locked doors, and accounting for all resources.

Computing in the new millennium is radically different. Abilities have been developed to obtain access into internal system resources, through potential breach in the security system. Organization's enterprise networks are not limited to few locations and few

employees but access is available to more and more employees and to customers. It gives information, product and services to general public also. Corporate Intranet is linked to Internet indirectly and in some cases directly. This envisages the need to have a Security mechanism for the interconnected computing resources, which is essentially a statement of management strategy as regards security. Organizations are, rightly concerned about the security implications of using the interconnected computing resources:

- a) Will hackers disturb internal systems?
- b) Will valuable organizational data be compromised (changed or read) in transit?
- c) Will the organization be embarrassed?

The interconnected computing resources of any organization are a vital resource that changes the way organizations and individuals communicate and do business. The inter connectivity between the computing resources offers enormous benefits in terms of increased access to information. However, the interconnectivity may cause significant and widespread security problems. Many agencies and organizations have been attacked or probed by intruders, with resultant losses to productivity and reputation. In some cases, organizations have had to disconnect from the interconnectivity temporarily, and have invested significant resources in correcting problems with the system and network configurations. Organizations that are unaware of or ignorant of these problems face the risk of being attacked by network intruders. Even organizations that do follow good security practices face problems due to new vulnerabilities in networking software and the persistence of some intruders. The fundamental inherent problems that are associated with a typical interconnected network are:

- Ease of eavesdropping and spoofing -- majority of traffic over the network, whether over the Intranet or Internet, is not encrypted. E-mail, passwords, and file transfers can be monitored and captured using readily available software.
- Vulnerable network protocol services -- a number of network protocol services are not designed to be secure and can be compromised by knowledgeable intruders; services used for testing are particularly vulnerable.
- Complexity of configuration -- host security access controls are often complex to configure and monitor; controls that are accidentally misconfigured can result in unauthorized access.
- Lack of policy -- many organizations are configured unintentionally for wide-open access without regard for the potential abuses from the external hackers and internal disgruntled employees. Quite a few organizations also permit more network services to the users than the users require for their operations and do not attempt to limit access to information about their computers. This could prove valuable to the intruders.

A business organization's interest in computer security is proportional to the perception of risk and threat. Many technical solutions are emerging to address these basic security concerns. However, they come at a price. Many of the solutions curtail functionality to increase security. Some require significant tradeoffs in terms of ease-of-use, while others cost traditional resources--staff time to implement and operate and money to buy and maintain the equipment and software. Many a times it is not considered how strong encryption-decryption methodology one is using, but the process of implementation, role, responsibility and constant ongoing monitoring becomes very important.

The Security Policy of any organization helps it to decide how an organization is going to protect itself. The policy will generally require two parts: a general policy and specific rules. The general policy sets the overall approach to Security by defining what is and what is not allowed. The rules may be supplemented with procedures and other guidelines. For any policy to be effective, the policy maker must understand the tradeoffs being made. The policy must synchronize with other related policy issues and provide a framework for linking high-level policy to detailed technical decisions and operational procedures.

## **2.0 Components of Security policy**

A typical security policy consists of the following components:

- Top level Security policy
- Security Architectural policy
- Security Operational policy.

It is required to understand each component completely, for an organization to have a structured approach for setting up a secured infrastructure. Each component forms a means for communicating procedures/policies to be followed in order to reduce the chance of any security breach to the end users.

### **2.1 Top Level Security Policy**

The Top Level Security policy is prepared by the Top-level management of an organization to evaluate and understand the need for selecting and setting a "general direction". These act as guidelines that have to be followed by an organization to mitigate the risks and implications of usage of interconnected computing resources; such as the Intranet, the Extranet and the Internet. These guidelines help in appropriate allocation of resources and delegation of responsibility at various levels of the organizational structure. This policy provides the blueprint for setting security policies and procedures for risk assessment of information as an asset followed by threat determination and implementation measures.

### **2.1.1 Information Asset**

In order to develop an effective information security policy, the information produced or processed by an organization must be categorized according to its sensitivity to loss or disclosure. Based on this categorization, the policy for allowing users to access information or for transmitting information can be defined. Most organizations use certain sets of information categories, such as "Proprietary," "For Internal Use Only," or "Organization Sensitive." The categories used in the information security policy should be consistent with the existing categories. Data must be broken into four classifications, based on sensitivity, with separate handling requirements: SENSITIVE, CONFIDENTIAL, PRIVATE, and PUBLIC. This standard data sensitivity classification system must be used throughout the organization. The designated owners of information are responsible for determining data classification levels, subject to executive management review. These classifications are defined as follows:

- SENSITIVE: This classification applies to information that requires special precautions to ensure the integrity of the information, by protecting it from unauthorized modification or deletion. It is the information that requires a higher than normal assurance of accuracy and completeness. Examples of sensitive information include organizational financial transactions and regulatory actions.
- CONFIDENTIAL: This classification applies to the most sensitive business information that is intended strictly for use within organization. Its unauthorized disclosure could seriously and adversely impact the organization, its stockholders, its business partners, and/or its customers.
- PRIVATE: This classification applies to personal information that is intended for use within organization. Its unauthorized disclosure could seriously and adversely impact the organization and/or its employees.
- PUBLIC: This classification applies to all other information that does not clearly fit into any of the above three classifications. While its unauthorized disclosure is against policy, it is not expected to have a detrimental effect on the organization, its employees, and/or its customers.

### **2.1.2 Risk Assessment**

In simple terms, a risk is realized when a threat takes advantage of a vulnerability to cause harm to the system. Security policy provides the baseline for implementing security controls to reduce vulnerabilities and thus the risk. In order to develop a cost effective security policy, certain levels of risk analysis must be performed to determine the required rigour of the policy, which will drive the cost of the security controls deployed to meet the requirements of the security policy. How rigorous this effort must depends on:

- The level of threat an organization faces and the visibility of the organization to the outside world
- The sensitivity of the organization to the consequences of potential security threats

- Legal and regulatory issues that may dictate formal levels of risk analysis

In the past, such cost estimation has been required as a part of formal risk analyses to support measurements of the ROI of security expenditures. As dependence on networks by businesses and government agencies has become more widespread, the intangible costs of security threats equal or outweigh the measurable costs. Information security management time can be more effectively spent ensuring the deployment of "good enough security" rather than attempting to calculate the cost of anything less than perfect security.

### **2.1.3 Threat Determination**

A threat is any circumstance or event with the potential to cause harm to an organization through the disclosure, modification or destruction of information, or by the denial of critical services. Threats can be non-malicious, through human error, hardware/software failures, or natural disaster. Malicious threats can be categorized on a scale ranging from rational (obtaining something of value at no cost) to irrational (destroying the information or reputation of others). Typical threats in a network environment include:

- Component Failure - Failure due to design flaws, or hardware/software faults can lead to denial of service or security compromises through the malfunction of a system component. Downtime of a firewall or false rejections by authorization servers are examples of failures that affect security.
- Information Browsing - Unauthorized viewing of sensitive information by intruders or legitimate users, which can occur through a variety of mechanisms: mis-routed electronic mail, printer output, mis-configured access control lists, group IDs, etc.
- Misuse - The use of information assets for other than authorized purposes can result in denial of service, increased cost, or damage to reputations. Internal or external users can initiate misuse.
- Unauthorized deletion, modification or disclosure of information - Intentional damage to information assets that result in the loss of integrity or confidentiality of business functions and information.

### **2.1.4 Implementation Measures**

Organizations have different levels of sensitivity to risk. Security policy needs to reflect the organization's particular sensitivity to various types of security incidents and prioritize security investments on those areas of highest sensitivity. There are two major factors that drive an organization's level of sensitivity.

The first factor is the consequences of a security incident. Almost all organizations have some level of cost sensitivity - security incidents can result in significant recovery and restoration costs even if no critical services are affected. However, means of transferring risk (such as insurance policies or contractual terms and conditions) may mean that a certain level of cost exposure does not change

the business bottom line. One important step towards determining the consequences is performing an information asset inventory. While it sounds simple, keeping an accurate inventory of what systems, networks, computers, and databases are currently in use is a complex task. Organizations should combine such an inventory with a data classification effort, where the information stored online is categorized by its importance to the goals or mission of the business.

The second factor is directly related to the political or organizational sensitivities. In some corporate cultures, the upper level management may feel that an article in the mainstream press highlighting a break-in at your agency or business is a major disaster. In more open environments, such as universities and scientific research communities, the management may feel that an occasional incident is preferable to any complete restriction on the flow of information or outside access. These factors need to be considered when determining organizational sensitivity to security incidents.

### **2.1.5 Continuous Review**

A security policy should be formulated and reformulated depending upon the changing scenario in the technology and the business arena. One old truism in security is that the cost of protecting yourself against threats should be less than the cost of recovering if the threat were to strike you. Without reasonable knowledge of what you are protecting and what the likely threats are, following this rule could be difficult.

## **2.2 Security Architectural Policy**

A Security Architectural policy is usually developed in accordance with the Top Level Security Policy. An Architectural policy would ideally consist of various components of the Security profile. Creating a Security Profile involves a thorough understanding of the existing and forthcoming trends in the security & trust sector, the exact requirements to fully constitute the security profile and then identify how to go about building the security profile. Policy creation must be a joint effort by technical personnel, who understand the full ramifications of the proposed policy and the implementation of the policy, and by decision makers who have the power to enforce the policy. A policy, which is neither implementable nor enforceable, is useless. Since a computer security policy can affect everyone in an organization, it is worth taking adequate care to ensure you have the right level of authority on the policy decisions. This tactical level planning within the organization ensures the proper understanding of the following issues:

### **Organizational Issues**

The goal of developing an official computer security policy is to define the organization's expectations of proper computer and network use, and the procedures to prevent and respond to security incidents. In order to do this, various aspects of the particular organization must be considered.

- Firstly, the goals and direction of the organization should be considered. For example, a bank may have very different security concerns from those of a university.
- Secondly, the site security policy developed must conform to existing policies, rules, regulations and laws that the organization is subject to. Therefore it will be necessary to identify these and take them into consideration while developing the policy.
- Thirdly, it is necessary to consider security implications in a more global context, unless the local network is completely isolated and standalone. The policy should address the issues when local security problems develop as a result of a remote site as well as when problems occur on remote systems as a result of a local host or user.

### **Responsibility Framework**

A key element of a computer security policy is making sure everyone knows his or her own responsibility for maintaining security. A computer security policy cannot anticipate all possibilities; however, it can ensure that each kind of problem does have someone assigned to deal with it. There may be levels of responsibility associated with a policy on computer security. At one level, each user of a computing resource may have a responsibility to protect his/her account. A user who allows his account to be compromised increases the chances of compromising other accounts or resources. System managers may form another responsibility level: they must help ensure the security of the computer system and Network managers may reside at yet another level.

It is also required to inform and communicate to the user of the computing resource, about the architectural policy. Users who do not adhere to this policy shall be warned and the corresponding line manager informed. A user who continues to ignore warnings may be removed from his function. In case the user violates Security policy either by hostile or non-hostile mode of attack, legal actions need to be initiated. The Security Architectural policy which helps in understanding the setting up of a security policy statement are grouped under the following headings:

#### **2.2.1 Information Security Policy**

An Information Security policy should consider the following elements in a comprehensive manner.

- All major information assets shall have an owner.
- The owner shall classify the information into one of the sensitivity levels (A classification system classifies information into four levels. The lowest (1), is the least sensitive and the highest (4), is for the most important data / processes), depending on legal obligations, costs, corporate policy and business needs. He/she is responsible for protection of this information.
- The owner shall declare who is allowed access to the data.
- The owner is responsible for this data and shall secure it or have it secured according to its sensitivity.

It is required to ensure protection of all information assets, so that the current computing environment may be quickly re-established following a disaster. For each information asset, the following information should be defined:

- Type: hardware, software, data
- General Support System or Critical Application
- Designated "owner" of the information
- Physical or logical location
- Inventory item number, where applicable.
- Data Categorization

### **2.2.2 Personnel Security Policy**

A typical Personnel Security Policy provides the framework, which specifies details regarding password control mechanism and the need to implement password expiration procedures to enhance security. It also spells information regarding various facilities that can prevent cracking into the computing resources either by running password checkers on system password files or running network sniffers that can cause breakage into other accounts, disrupt service, abuse system resources, misuse email, examine other users restricted files, download PC binaries, copy unlicensed software or allow other users to copy unlicensed software.

### **2.2.3 Physical and Environmental Security Policy**

A Physical Security policy document should exist detailing the measures taken to protect buildings safes, computer rooms & wiring cabinets from disasters like (flooding, fire, earthquakes, explosions, power outage), theft access control. Creating or earmarking zones with different levels of priority is done to restrict any unforeseen hazards.

### **2.2.4 System Administration Policy**

The System Administration policy helps in ensuring that the systems are available when needed and that confidential information is only available to those provided with authorized access and that the information is not subject to unauthorized changes.

### **2.2.5 Network Policy**

The Network Policy guidelines are needed to make sure that the network is secure and various Intrusion Detection measures are implemented in the network to prevent unauthorized access. It helps in monitoring and mitigation of risk. The Network Administrator must maintain an inventory of production information systems that indicates all existing hardware, software, automated files, databases and data communications links.

## **2.2.6 Application Development Policy**

Security should be an integral part of new systems. When functional requirements are designed, security requirements should be formulated corresponding to the sensitivity and availability of data to be handled by the system. This is handled in the Application Development Policy.

## **2.2.7 General Technical Guidelines**

This general guideline should contain the recent information and development about the viruses and anti-viruses respectively. It should also contain the policy related to the password, usage of floppies by various applications and outside connectivity with the clear guidelines when it can be used and how.

## **2.3 Security Operational Policy**

A Security Operational policy should address the following Security Policy issues.

### **2.3.1 Who is Allowed to use the Resources?**

A step that must be taken for developing security policy is defining who is allowed to use the systems and services. The policy should explicitly state who is authorized to use what resources and at what time.

### **2.3.2 What is the Proper Use of the Resources?**

After determining who is allowed access to system resources, it is necessary to provide guidelines for the acceptable use of the resources. A set of guidelines has to be established for different types of users. The policy should state what are the acceptable use as well as unacceptable uses. It should also include types of use that may be restricted and must define limits to access and authority. It is required to consider the level of access various users will have and what resources will be available or restricted to various groups of people. The policy should clearly state that individual users are responsible for their actions. Their responsibility exists regardless of the security mechanisms that are in place. It should be clearly stated that breaking into accounts or bypassing security is not permitted. The following points should be covered when developing an acceptable use policy:

- Is breaking into accounts permitted?
- Is cracking passwords permitted?
- Is disrupting service permitted?
- Should users assume that a file being world-readable grants them the authorization to read it?
- Should users be permitted to modify files that are not their own even if they happen to have write permission?

- Should users share accounts?

It is required to incorporate a statement in the security policies concerning copyrighted and licensed software. Licensing agreements with vendors may require some sort of effort on the organization part to ensure that the license is not violated. In addition, it is necessary to inform users that the copying of copyrighted software may be a violation of the copyright laws, and is not permitted. For copyrighted and/or licensed software, it is specifically required to include the following information:

- Copyrighted and licensed software may not be duplicated unless it is explicitly stated that you may do so.
- Methods of conveying information on the copyright/licensed status of software.
- When in doubt, DON'T COPY.

An acceptable use policy is very important. A policy that does not clearly state what is not permitted may leave you unable to prove that a user has violated the policy.

### **2.3.3 Who Is Authorized to Grant Access and Approve Usage?**

The Security policy should state who is authorized to grant access to the information computing resource services. Further, it must be determined what type of access they are permitted to give. If you do not have control over who is granted access to your system, you will not have control over who is using your system. Controlling who has the authorization to grant access will also enable one to know who was or was not granting access if problems develop later. There are many schemes that can be developed to control the distribution of access to your services. The following are the factors that one must consider when determining who will distribute access to the resources:

#### **Distributing Access**

Sometimes it is required to have a centralized distribution point to a distributed system where various sites or departments independently authorize access. The trade off is between security and convenience. The more centralized, the easier to secure.

#### **Creating Accounts and Terminating Access**

From a security standpoint, one needs to examine the mechanism that is used to create accounts. In the least restrictive case, the people who are authorized to grant access would be able to go into the system directly and create an account by hand or through vendor supplied mechanisms. Generally, these mechanisms place a great deal of trust in the person running them, and the person running them usually has a large amount of privileges. It is required to select someone who is trustworthy to perform this task. Specific procedures must be laid down for the creation of accounts. These procedures should be well documented to prevent confusion and reduce mistakes. Security vulnerability in the account authorization process is not only possible through abuse, but is also possible if a mistake is made. Having clear and well-documented procedure will help ensure

that these mistakes don't happen. It is required to communicate these procedures to the people who will be following them and make sure that they understand them.

The granting of access to users is a potential source of vulnerability. Hence the selection of an initial password should be one, which cannot be easily guessed. It is required to avoid using an initial password that is a function of the username, is part of the user's name, or some algorithmically generated password that can easily be guessed. In addition, one should not permit users to continue to use the initial password indefinitely. If possible, one should force users to change the initial password the first time they login. It should be considered that some users may never even login, leaving their password vulnerable indefinitely. Some sites choose to disable accounts that have never been accessed, and force the owner to reauthorize opening the account.

#### **2.3.4 Who May Have System Administration Privileges?**

One security decision that needs to be made very carefully is who will have access to system administrator privileges and passwords for the computing resources and services. Obviously, the system administrators will need access, but inevitably other users will request special privileges. The policy should address this issue. Restricting privileges is one way to deal with threats from local users. The challenge is to balance restricting access to these to protect security with providing privileges to people who need access in order to perform their tasks. One approach that can be adopted is to grant only enough privilege to accomplish the necessary tasks.

Additionally, people holding special privileges should be accountable to some authority and this should also be identified within the site's security policy. If the people who have been granted privileges are not accountable, one runs the risk of losing control of the computing resource and will have difficulty in managing a compromise in security.

#### **2.3.5 What Are The Users' Rights and Responsibilities?**

The policy should incorporate a statement on the users' rights and responsibilities concerning the use of the site's computer systems and services. It should be clearly stated that users are responsible for understanding and respecting the security rules of the systems they are using. The following is a list of topics that you may wish to cover in this area of the policy:

- What guidelines should one have regarding resource consumption (whether users are restricted, and if so, what the restrictions are)
- What might constitute abuse in terms of system performance
- Whether users are permitted to share accounts or let others use their accounts.
- How "secret" users should keep their passwords.
- How often users should change their passwords and any other password restrictions or requirements.
- Whether you provide backups or expect the users to create their own.
- Disclosure of information that may be proprietary.

- Statement on Electronic Mail Privacy
- A policy concerning controversial mail or postings to mailing lists or discussion groups (obscenity, harassment, etc.).
- Policy on electronic communications: mail forging, etc.

There is a tradeoff between a user's right to absolute privacy and the need of system administrators to gather sufficient information to diagnose problems. There is also a distinction between a system administrator's need to gather information to diagnose problems and investigating security violations. The policy should specify to what degree system administrators can examine user files to diagnose problems or for other purposes, and what rights have been granted to the users. It is required to make a statement concerning system administrators' obligation to maintaining the privacy of information viewed under these circumstances. A few questions that should be answered are:

- Can an administrator monitor or read a user's files for any reason?
- What are the liabilities?
- Do network administrators have the right to examine network or host traffic?

### **2.3.6 What To Do With Sensitive Information?**

Before granting users access to the computing resources and services, one needs to determine at what level one has to provide for the security of data. By determining this level of sensitivity of data that users store on their systems, one can provide for various means for the users to store very sensitive information on a system that is not so secure. The mode of storage appropriate for the storage of sensitive information can include storing of data in different ways (disk, magnetic tape, file servers, etc.).

### **2.3.7 What Happens When the Policy is Violated?**

It is obvious that when any type of official policy is defined, be it related to computer security or not, it will eventually be broken. The violation may occur due to an individual's negligence, accidental mistake or because of not having been properly informed of the current policy, or not understanding the current policy. It is equally possible that an individual (or group of individuals) may knowingly perform an act that is a direct violation of the defined policy.

When a policy violation has been detected, the immediate course of action should be pre-defined to ensure prompt and proper enforcement. An investigation should be performed to determine how and why the violation occurred. Then the appropriate corrective action should be executed. The type and severity of action taken varies depending on the type of violation that occurred.

## **Determining the Response to Policy Violations**

Violations to policy may be committed by a wide variety of users. Some may be local users and others may be from outside the local environment. Sites may find it helpful to define what it considers "insiders" and "outsiders" based upon administrative, legal or political boundaries. These boundaries imply what type of action must be taken to correct the offending party; from a written reprimand to pressing legal charges. So, not only does one need to define actions based on the type of violation, one also needs to have a clearly defined series of actions based on the kind of user violating the computer security policy. Though these seem rather complicated, they should be addressed long before it becomes necessary as the result of a violation.

One point to remember about the security policy is that proper education is the best form of defense. For the outsiders who are using the computing resources legally, it is the organization's responsibility to verify that these individuals are aware of the policies that has been set forth. Having this proof may assist in the future if legal action becomes necessary.

As for users who are using the computing resources illegally, the problem is basically the same. What type of user violated the policy and how and why did they do it? Depending on the results of the investigation, in case of a security breach or trust violation, one must try to "plug" the hole in computer security and chalk it up to experience. Or if a significant amount of loss was incurred, then drastic action against the culprit has to be initiated.

## **Local Users Violate the Policy of a Remote Site**

In the event of a local user violating the security policy, the management should have a clearly defined set of administrative actions to be taken against that local user. These situations involve legal issues, which should be addressed when formulating the security policy.

Whenever the computing resources suffer an incident, which may compromise computer security, the strategies for reacting may be influenced by two opposing pressures. If management fears that the computing resource is sufficiently vulnerable, it may choose a "**Protect and Proceed**" strategy. This approach will have as its primary goal the protection and preservation of the site facilities and to provide for normalcy for its users as quickly as possible. Attempts will be made to actively interfere with the intruder's processes, prevent further access and begin immediate damage assessment and recovery. This process may involve shutting down the facilities, closing off access to the network, or other drastic measures. The drawback is that unless the intruder is identified directly, they may come back into the site yet again via a different path, or may attack another site.

The alternate approach, "**Pursue and Prosecute**", adopts the opposite philosophy and goals. The primary goal is to allow intruders to continue their activities at the site until the site can identify the responsible persons. This approach is endorsed by law enforcement agencies and prosecutors. The drawback is that the agencies cannot exempt the management from possible user lawsuits if damage is done to their systems and data. If the culprit is an employee of the organization, it may choose to take disciplinary actions. The computer security policy needs to spell out the choices and how they will be selected if an intruder is caught. Careful consideration must be taken by the

management, regarding their approach to such issues, before the actual problem does occur. The strategy adopted might depend upon each circumstance. Or there may be a global policy, which mandates one approach in all circumstances. The pros and cons must be examined thoroughly and the users of the facilities must be made aware of the policy so that they understand their vulnerabilities no matter which approach is taken.

### **3.0 Conclusion**

Understanding the business needs of an organization would allow the rapid development and deployment of a Security policy, which conforms to the culture and strategic outlook of an organization. The framework so evolved would allow the assessment of risk, vulnerability, and threat, besides providing the necessary leeway for contingency planning and ensuring utmost physical security. The above framework critically evaluates the existing security flaws and helps in mitigating the security risks and provides necessary corrective actions to eliminate such flaws and security hazards.

Based on the above framework, an IT security policy can be constructed. Here are the five criteria for evaluating any policy:

- Does the policy comply with law and duties of third parties?
- Does the policy unnecessarily compromise the interest of the employee, the employer or third parties?
- Is the policy workable practically and can be enforced?
- Does the policy deal appropriately with all different forms of communications and record keeping in the office?
- Has the policy been announced in advance and agreed to by all concerned?

Therefore it is required to communicate to all the users in the information chain, reasonable knowledge of what information the organization is trying to protect and what are the likely threats an organization has to face.

#### **Interpreting the Policy**

It is important to define who will interpret the policy. This could be an individual or a committee. No matter how well written, the policy will require interpretation from time to time and this body would serve to review, interpret, and revise the policy as needed.

#### **Publicizing the Policy**

Once the Security policy has been written and established, a vigorous process should be engaged to ensure that the policy statement is widely and thoroughly disseminated and discussed. A mailing of the policy should not be considered sufficient. A period for comments should be allowed before the policy becomes effective to ensure that all affected users have a chance to state their reactions

and discuss any unforeseen ramifications. Ideally, the policy should strike a balance between protection and productivity. Meetings should be held to elicit these comments, and also to ensure that the policy is correctly understood. These meetings should involve top-level management as well as low-level employees as security is a collective effort. In addition to the initial efforts to publicize the policy, it is essential for the site to maintain a continual awareness of its computer security policy. Current users may need periodic reminders. New users should have the policy included as part of their probationary training package. As a condition for using the computing resources and facilities, it may be advisable to have them sign a statement that they have read and understood the policy. Should any of these users require legal action for serious policy violations, this signed statement might prove to be a valuable aid.

Essentially the old truism in security, “ the cost of protecting yourself against a threat should be less than the cost recovering if the threat were to strike you” should be kept in mind.

## **References:**

1. IDRBT's Working Paper on “Construction of Security Policy for Banks”, by V P. Gulati, K.R. Ganapathy, Ashutosh Saxena & M.V.S. Prasad.
2. “Handbook of Information Security Management”, by Micki Krause and Harold F. Tipton, 1998, Auerboch Publications, CRC Press.
3. “Information Security Management: A Hierarchical Framework for Various Approaches”, M. M. Eloff & S. H. Von Solms, Computer and Security, Vol. 19, 2000, Pages 243 – 256.
4. Deborah Russell & G. T. Gangemi Sr., “Computer Security Basics”, O'Reilly & Associates, Inc, 1991.