Developing a Security Policy

The purpose of this paper is to discuss some of the special issues which in developing a security policy for an organization. In general, an organization’s security policy should be the basis for its information security program. Information is a valuable business asset to an organization that should be kept private and protected. I believe that the very first thing to do for protecting information is to set up stern security policies and yet flexible enough to accommodate changes to the industry. Creating a set of security policy to safeguard and control information can be a time consuming mission that involves a lot of attention and planning. Therefore, in developing a successful security policy, it is necessary for management of the organization to follow certain principals that were acknowledge in the article.

Introduction

Organizations face security threats from a wide range of sources and are vulnerable to attacks such as computer viruses and hacking. Information security that relies only on technical means is not sufficient and needs to be supported by policies and procedures. Management is suppose to clearly express what the security policy actually justify. Besides protecting information, a well written and implemented policy should also protect employees and customers of the organization. Depending to the company’s size and resources, management implementing a security policy needs to find the right balance between overreacting and vulnerable of exposing their system to threats.

General outline of Security Policy

The objective of a security policy is to translate and clarify management’s position on security issues and safeguard information from both inside and outside the organization.
Each paragraph should clearly state who is responsible for this policy at every level within the company, who and what are protected by the policy and who must adhere according to the policy. And again, management should have scope on what is not covered in the policy.

**Policy flexibility and management**

An security policy is a "living" document and should be flexible enough to change often. An organization should not be caught in a specific policy as the industry changes rapidly. It is important to monitor and review the policy continuously for improvement as new threats are being discovered. This includes changes in the organization resulting in new threats. Functions of the organization have to be modified as necessary to minimize any new threat introduced. As time goes by, it is crucial to manage the relevancy of the security policies. New policies may be added when needed; obsolete policies must also be taken off.

**Roles and Responsibilities**

One of the first things that everyone needs to know is; what are their responsibilities under this policy? There are basically two types of responsibilities, Organizational and Functional. Organization responsibilities involves individual which holds higher position such as the President and the Vice President. Functional responsibilities cover Managers and Chief Officers. It is important to include roles and responsibilities for various individual with the organization and external agents that are involved in the organization business functions.

**Compliance and Enforcement**

The article that was written by JoelWeise has failed to mention on the issue of compliance and enforcement of the security policy. This part of the policy have to explain what happens if the policy is not followed. It is necessary to develop a
method to measure compliance with the policy. The best person to perform this task cost effectively is the internal auditors to ensure all employees understand and aware of the policies. The policies must be enforced in a strictly manner and people not following the rules should be punished. Once a culprit is identified, the organization should choose to take actions spelt out in the security policy.

**Risk Management**

This issue is probably the largest section of the security policy as it has many elements to cover. Risk management should not be overlooked, nor ignored, it is necessary that security policies reflect realistic business goals and values. Risk management is a continuous process and must be reevaluated whenever changes occur to the organization. In the process of identifying the risk, it is significant to remember to rank the risks by level of severity and priority. This ensures that we make wise cost-effective decision and should not spend more to protect something than is not worth on.

**ISO 17799**

ISO 17799 is a comprehensive set of information security policies maintained by the Information Standards Organization. It can be thought of as the “holy grail” of information security standards and can be used minimally as a standard against which to measure the policies developed by organizations. The ISO 17799 defines 127 security controls which are grouped into 10 sections that can be used as a security checklist to assist organizations in defining their policy. As part of the preparation process, a questionnaire consisting of all relevant securities controls defined in ISO 17799 is created. A checklist is designed according to the recommended best practice from ISO17799 and at the same time gather data whether it is being implemented in the organization.
**Conclusion**

The basic goals of security are availability, confidentiality and integrity. Organizations must determine what they need to protect, what threats they are protecting it from and how to protect it. A security policy is the foundation and crucial step in which security is built in an organization. As with any foundation, it must be well designed, and well constructed; it can then be trusted to support the organization functions and business processes.

**References**

