Security Policy: Enforcement and Compliance

Security policy is the basis of organization's information security. Many organizations have information security policy in place to ensure that their information is always secure. However, having a security policy document in itself is not enough. It is very important to ensure that the contents must be implemented to be effective. This article provides some recommendations on the systematic approach for policy enforcement and compliance.

The following steps are suggested for achieving policy enforcement and compliance:

- **Implementing Security Awareness Program**

The key to compliance with security policy is education. Educating users on the need for security is important as it will help users to understand the importance of information security, and how it will benefit them in their daily works. Thus, implementing a security awareness program is a major step in ensuring compliance with security policy.

In order to make security awareness program effective, it is crucial to have a strategy on building a solid program. An effective security awareness strategy will ensure that all users are aware of:

- the existence of security policy;
- where to find it;
- how to comply with it;
- how it will aim to improve the operations of the company;
- how vital the protection of information really is; and
- the consequences of non-compliance.

The program should emphasize on explaining why "Security is everyone's responsibility" and teach the users about their role in maintaining the security. This is because people often tend to think that only the IT department or Information Security personnel can and need to take care of information security issues and it is not their responsibility to participate in protecting the security of their company.

- **Communicating policy effectively**

Once security policy has been established, it must be communicated formally to all the people responsible for enforcing and complying with it. This should include employees, vendors, contractors, and other relevant users. Given the nature of the organization, it may also be necessary to communicate some or all policies to customers as well.

The endorsed final copy of security policy must be made easily available to all users. There are some ways to distribute the policy to the users. Security Policy can be introduced to the users during new orientation and incorporated into the company's Employee Handbook as a code of practice for employees. It can also be published onto

the company's intranet which available to all employees for download, printing, and saving. Users are to acknowledge that the policy is read and understood by signing and agree to comply with it.

An essential part in this communicating process is to establish a record that those involved have read, understood, and agreed to abide by the policy. It is a big challenge to ensure that users understand and accept the policy that governs them. Policy acceptance is always dependent on the policy's inherent ability to describe acceptable and/or unacceptable behavior with respect to information systems security. A clear, concise, coherent, and consistent policy is more likely to be accepted and followed.

- **Checking for compliance**

How well does your user and technology comply with your written policy? A method to measure compliance with the policy should be established. This may include a compliance assessment on a regularly scheduled basis to evaluate the effectiveness of current security policy. The auditors who are responsible for checking the compliance with the security policy should be independent of the persons implementing the policy. In checking user compliance, auditors need to ensure that all users are aware, understand and perform their roles and responsibilities as stated in the policy. For technology compliance, the audit should focus at technical security settings of network, operating systems as well as other critical systems and applications.

- **Monitoring**

The monitoring process is important as new threats and technologies appear due to the changing environment and operations of the organization. Risk assessment process that was conducted at the beginning of the policy development phase should be reviewed again and controls have to be modified as necessary for any new threats introduced. It is crucial to review the security policy continuously to maintain the relevancy of the content. The frequency of review will depend upon the nature of the policy. New policy must also be added when necessary and obsolete policy must be removed.

Conclusion

Security policy is the foundation of information security in an organization. As with any foundation, it must be well developed, enforced and complied with to improve the security of information, from both inside and outside the organization. Compliance with the security policy is not an easy task as it involves translating the written policy into actions. It requires careful planning and participations of all the related parties.