The Importance of Setting up an Information Security Management Committee in Organization

One of the management responsibilities in ensuring the effective implementation of Information Security Management System (ISMS) in organization is by setting up an Information Security Management Committee. This has been briefly said in the article titled “Information Security Management System (ISMS) Implementation: Examining Roles and Responsibilities” in the last published newsletter. This article will explain further the importance of the committee in achieving organization’s goals in implementing effective information security.

Who should be in the Information Security Management Committee?

An Information Security Management Committee is generally composed of representatives from departments within the organization. Representatives include members from the department of Information Security, Internal Audit, Risk Management, Physical Security, Information Systems, Human Resources, Legal, Finance, and Accounting Departments, as well as various user departments. The committee is generally made up of individuals who have relevant expertise, who are seen as influential in the information security area, and who can represent their own department or area of expertise.

Importance of Information Security Management Committee

Experience has shown that the following factors are often critical to the successful implementation of information security within an organization:

- Information security policy, objectives, and activities that reflect business objectives;

- An approach and framework to implementing, maintaining, monitoring, and improving information security that is consistent with the organizational culture;

- Visible support and commitment from all levels of management;

- Effective marketing of information security to all managers, employees, and other parties to achieve awareness.

All the critical success factors support the importance of setting up the Information Security Management Committee that emphasize on the criticality of having inputs from all the departments throughout organization. The inputs from various departments are important to achieve the following goals:

- To identify the changes in organizations accurately

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware security mechanisms. The process of establishing, implementing, monitoring, reviewing and improving these controls requires organization to continuously identify and take care of all the changes in the business environment, security threats, industry best practices and legal requirements. This is to ensure that specific security and business objectives of the organization are met and the process should be done in conjunction with other business management processes. To accurately identify and understand all the changes that organizations are facing, inputs from all departments throughout organization are important.

- To bridge the divide between management and technical

  Management has specific goals for the organization, and sometimes technical people are not in the position to understand these nuances. Both groups should understand that security is not something that can be wrapped in a package and bought off the shelf. It should be a goal that both parties strive to maintain. One of the ways to bridge the divide is by setting up an Information Security Management Committee.

- To segregate responsibilities in implementing information security

  There is always a misconception on the responsibilities of implementing information security in organization. The popular belief is that it is the responsibilities of Information Security Department alone in ensuring that organization's information is always secure. However, this is absolutely not right. In implementing information security, some tasks should be performed periodically including:

  - Review the current status of information security
  - Review and monitor security incidents
  - Approve and review information security projects
  - Approve new or modified information security policies
  - Perform other information security management related activities

  All the tasks need commitment from various departments to be enforced throughout the organization.

Conclusion

Information security management committee is an important part of the success of information security implementation in organization. Organization should prioritize the formation of this committee to ensure that the implementation of information security in their organization achieve the organization's goals.