Infosecurity Management

Dr D S Kushwaha[1], (Dr) A S Vidyarthi[2]

[1]Professor, R C Institute of Technology, New Delhi (India)

[2]Director, Institute of Engineering & Technology, Lucknow (India)

Abstract: ***Management of Information security is a business issue. The information security status in an organizational need has two levels of measurements. The first level is a high level measurement focusing on business and management processes. The second level is the technical and more detailed measurement of information security controls. Security measures need to be implemented to prevent unwanted security breaches. Determining the level of information security in an organization is easier said than done. Information security levels need to be measured on a technical and in-depth level. There is, however, a need to measure information security on a higher level, namely the management and business process level. The information security culture and the climate in an organization are very important concepts, which could affect the implementation of information security.***

Keywords: Infosecurity, stages or levels, security policy, security concepts

1. Introduction

Security breaches can cost an organization millions! Information security business and management processes as well as an information security culture need to be in place before in-depth and detailed controls could be implemented. Both the business and technical levels of security in an organization need to be measured to determine future actions in securing information. A framework in which to do the measurement of information security levels in an organization is thus needed to ensure an effective and efficient management and measurement of information security management. Information security in an organization needs to be quantified to determine what level of security is implemented in the organization and what aspects still require attention, and to track the progress of the implementation of security measures. When implementing information security, it is important to understand that security does not only imply technical controls, but also management processes and business processes

2. Standard

Information security in an organization needs to be quantified to determine what level of security is implemented in the organization and what aspects still require attention, and to track the progress of the implementation of security measures.
Therefore, an organization should first measure its business processes and information security concepts on a high level before starting to implement firewalls everywhere. Having these processes in place will automatically lead to the implementation of the more technical and detailed controls.

3. Framework

(i) Information Security
When an organization initiates the process of implementing information security, or after the implementation has been done, there is a certain level of information security in the organization. This information security level will indicate the organization's position and what the organization still needs to do. The following model indicates the different progressive *stages or levels* through which an organization should go when implementing information security management.

(ii) Current status
An organization's current level of information security management needs to be determined. It could be that the organization has never implemented information security before. The organization could also be in the process of implementing information security. This level of security needs to be measured.

(iii) Level one
The first level that needs to be measured is the management and business process in the organization. The management and business process focuses on management's commitment to, and support of information security processes in the organization. Implementation will be successful only when management is committed to and supports the information security processes in the organization.

By paying attention to the business issues first, the organization's employees can be prepared for the changing process of implementing information security. This level of information security needs to be measured to determine whether the organization can proceed on to more detailed and technical implementations.

- Culture
- Management
- Standards, procedures and policies
- Risks

(iv) Level two
On the second level, the organization needs to map the procedural and technical controls to be implemented in the business and management processes. BS7799 can once again be used, but in this stage, the complete standard needs to be covered. This implies that both the detailed business processes and procedures such as the issuing of passwords, as well as the technical controls such as the implementation of firewalls and encryption are addressed.

(v) Security Management

After the implementation of management and business processes as well as the in-depth, procedural and technical implementation of security, the organization can be certain that information security management is fully covered.

4. Level One: High Level

The focus of this research is on the first level, namely the management and business process of information security management. It will in other words also focus on the information security culture in the organization. To measure information security on a high-level, the organization can make use of a survey.

Measuring information security on a management and business level comprises some components, which need to be measured on a high level, meaning that the focus should not be on detailed processes.

The following components were identified and used to develop the questionnaire:

(i) Management: Management plays a crucial role in the process of implementing information security by assuring that the resources under its authority are protected. In order to implement information security successfully, management must give its support. The perceptions and attitude of management towards information security has an important effect on employees' behavior and how they will respond to the implementation of information security. In level one, management's support and role in the information security process are issues that should be measured.

(ii) Policy: The information security policy is the heart of the organization.

(iii) Awareness: There will be no benefit to an information security policy or controls if no one is aware of it. Awareness of information security concepts, the policy and the need for information security are some of the issues covered on level one.

(iv) Training and Education: Employees need to be educated about the security aspects required in the information security policy.

(v) Culture and Change: When an organization starts to implement information security it involves change. To implement information security the organization's corporate culture plays a significant role.

The information security corporate culture can be achieved through management's example, support and commitment, by having an information security policy and by enforcing the awareness of the policy and information security issues.

An Information Security Culture that could prevent internal security breaches through proactive actions would lead to continuous improvement and evaluation of Information Security.

5. Conclusion

Issues covered on level one is for instance, whether information security is viewed as important and whether the management style is open to the changing processes involved in implementing information security. By following a structured approach in measuring the levels of information security, an organization can be assured that information security is implemented effectively and efficiently. By using a tool such as the developed questionnaire, the organization can measure security on level one and progressively implement information security.

References

[1] Information Security Magazine, Issue 46.

[2] Eloff, M.M., Von Solms, S.H. 2000, A Computers & Security.

[3] A Network Security. Issue 3. Computer Security Handbook.

[4] Health care management and information systems security, Issue 2.

[5] Implementing Information Security in the 21st century, Issue 4.