

INFORMATION SECURITY A BOON FOR ORGANIZATIONS

Supreet Kaur
Assistant Professor
IT Department

Sri Guru Tegh Bahadur Institute of Management and Information Technology, New Delhi, India

Abstract : This paper discusses the importance and concept of information security knowledge among the employees of an organization. It is nowadays a necessity to make them implement the information security practices in their day to day work routine, which would improve the overall security environment of the organization.

Information security controls are defined in this paper. How they can be implemented in increasing the information security level is also discussed along with their types.

Set of guidelines is presented to determine the information security profile of an organization, which makes sure that no assumptions are to be made, in aspect of information security. This thus, leads towards a secured organization.

Index Terms – Information threats, information security, controls, guidelines.

I. INTRODUCTION

The importance of information security education, training and awareness, cannot be denied. In today's organizations it is a necessity for employees to make information security decisions, cautiously, while performing their work duties.

It has always been a myth that employees of an organization play important role, in the information security network. But. The truth is that their impact on security network is only dependent upon their ability to make wise decisions, in terms of information security when the need arises. Now this intelligent behavior amongst the employees of an organization can only be achieved if they are aware of the threats that lack of information security can cause.

It is necessary to define what information is in today's industry. Information can be termed as a result that one gains from an analyzed data. This data is composed of the structured records that employees of an organization store as database, spreadsheets, documents etc.

Thus, the basic security knowledge is a must for every employee which includes, making them learn the information security tasks in terms of protection, detections, solutions etc.

The need of information security became more prominent in 1996, when an information security survey, performed by Department of Trade and Industry, concluded that negligible number of small to medium sized organizations ignored the threat to their information and thus did not perform a proper risk analysis.

To summarize, it can be said that the effort of every single employee in information security practices will help the information security management team to develop and to redesign a more functional and appropriate security practice among its organization members. Hence, it is now mandatory to present set of security controls and principles that should be implemented under most of the circumstances. This would enable organizations to reach a minimum level of information protection, which would be adequate under day to day conditions, without conducting an expensive exercise of risk analysis.

II. RELATED WORK

Rossouw Von Solms and Helen Van De Haar, presented in their paper a research on a new development that is establishment of information security baselines, which included set of security controls that can be installed in most of the circumstances. They analyzed number of manuals bases on these baselines and came to a conclusion that the extensive set of controls offered, can become very detailed for an organization and hence it loses the advantage of security baselines. Thus, they came up with their own baseline method to provide information security in an organization that provides minimum level of protection. [1]

Eric Amankwa, Marianne Loock and Elmarie Kritzinger presented an investigation in their paper. They did investigate the basic difference between information education, training and awareness. The data collected through their investigations was analyzed and they defined a working definition of information security. [2]

Omar Zakaria, discussed the basic security knowledge concept in his paper. In the later part of his paper he presented the concept that was based on how organization members can possess basic information security knowledge. [3]

III. INFORMATION SECURITY CONTROLS

Information security control can be defined as measures taken to detect, response, avoid or reduce the security risks to an organization's information. These controls are termed as technical controls based on their nature. They include the authentication of a user, access control, firewalls etc.

These controls can be categorized into mainly three categories that are the following [2] :-

1. Preventive information security control:
These are used to basically avoid the threats to organization's information. For example, the controls can include the antivirus software's that can protect information to be accessed by an unauthorized user.
2. Detective information security control:
These come into play when information system of an organization is affected by a threat. For example, if an unauthorized user is successful in breaking into the information system of an organization, software can be developed that would notify the information security management team through a mail to take necessary measures.
3. Corrective information security control:
Now these controls are basically installed to limit the extent of the damage that has been done to the organization's information system. for example, to redesign the information management system to increase the security level to bring the organization to its normal working environment.

IV. GUIDELINES TO INFORMATION SECURITY

In today's industry there's a lack of information security knowledge among the employees of an organization. Thus the following guidelines should be followed to improve the level of information security environment [3]:

1. Conducting information security knowledge sharing sessions:
Regular sessions should be held in an organization involving all the departments. Every employee should participate in these sessions. This would help everyone to understand the risks that the information system of the organization is exposed to. Sharing of daily information security issues would help all the employees to perform in an appropriate manner at the time of information crisis.
2. Documentation of information security knowledge:
The knowledge shared in the information security sessions should be documented. Also the practices performed, their results, policies presented by information security management department should be a part of this documentation.
3. Monitoring of information security environment:
Information security in an organization's environment should be monitored regularly. This would ensure that preventive measures can be taken against any threats to the information of the organization.
4. Information security measures implemented by employees:
The implementation of measures towards the security of the organization's information should be analyzed and evaluated on regular basis. It should be investigated that the employees of the organization are well informed about the measures and implementing them in their everyday work routine.

V. CONCLUSION

An organization's security is one of the major concerns in today's industry. Government is spending a huge amount in ensuring that their nation's information is well secured and not exposed to threats.

It thus is a necessity of every organization to educate their employees in terms of information security measures. This would ensure that each employees of the organization will implement the information security measures in their day to day work routine. This paper did include some of the information security controls that can be a part of any industry's organization. These controls when installed would improve the level information security measures adopted.

Also some guidelines are listed that an organization should implement which makes sure that every employee is well educated and trained in aspects of information security measures. The guidelines should be a part of policies of the organization so that it is secured towards the risks to the information of the organization.

REFERENCES

[1] Eric Amankwa, Marianne Loock, Elmarie Kritzinger, 2014. A Conceptual Analysis of Information Security Education, Information Security Training and Information Security Awareness Definitions. The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)

[2] Rossouw Von Solms And Helen Van De Haar, 2000. From Trusted Information Security Controls to a Trusted Information Security Environment. International Federation for Information Processing 2000

[3] Omar zakaria, 2006. Internalisation of Information Security Culture amongst Employees through Basic Security Knowledge. International Federation for Information Processing, Volume 201

