RESEARCH ARTICLE OPEN ACCESS

Information Security Management of an organization with a focus on Human perspective

Karandeep Kaur
(Department of Computer Science, Guru Nanak Dev University, Amritsar)

----------**********----------

Abstract:

The dynamic nature of Information security scenario these days due to the popularity of online businesses has posed a daunting challenge to the organizations security paradigm. Organizations are looking for new policies to be implemented to provide the best possible security mechanism. However, they tend to ignore the human side of the security compliance measures. Every piece of information that has been secured using various technologically advanced policies has to be accessed ultimately by the employees of the organization. Their attitude and commitment to safeguard the interests of the organization plays a significant role in all measures being taken for information security. Humans and technology has to play an integrative part in order to guarantee the safety of information assets. This paper reviews the existing literature of information security management in a comprehensive manner focusing on the role of top management and employers for effective security measures.

Keywords **— Information Security, Role of Humans, Top Management, Employees, Information Security Management.**

----------**********----------

I. INFORMATION SECURITY MANAGEMENT

Internet and online businesses have brought new avenues for organizations for expansion and progress. However, the most critical asset of an organization i.e. information, becomes vulnerable in such systems. Information security management thus comes into the scenario. Likewise, the design of information security policies and its compliance also becomes significant in organizations. There have been researchers working on this part and proposing new technologies, security mechanisms and policies which are being followed by organizations world-wide. Though a lot of work has been done in the technology advancement context, but a little focus has been given to the human aspect of information security. Managers or employees are the ones who deal with the information on every-day basis. They need to play closely with the information security management mechanism. Their roles, practices and its significance have been considered in this paper. It will provide an insight into the suggestions given by various researchers in this perspective.

In online businesses, security is the biggest concern as the number of security breaches and thefts are increasing day-by-day. Such breaches result in huge financial as well as goodwill losses for the organizations. Credit card information as well as other personal data is compromised in case of poor security policies. This brings about loss of customer's trust in such businesses and influences the business in a negative manner. The literature study shows the causes of data breaches. Jaeger (2013) says that 38% of data breaches were caused due to lost paper files, 27% due to mislaid portable memory devices and only 11% were caused due to outsiders and hackers. Malicious intent of the insiders was equally responsible for data breaches. Violation of access policies also contributes to weak security of the organization. Hence, it is observed that the human link is the weakest one in

the system of information security. Therefore, the organizations must have rigid security policies and need to inculcate the information security culture and awareness in the employees.

II. THE HUMAN PERSPECTIVE

Looking at Information security from the human perspective reveals interesting facts and figures. The role played by top managers and employees along with the training programs is discussed in the section below.

A. ROLE OF TOP MANAGEMENT

Many policies and technical approaches have been developed and adopted by various organizations, but this has not been enough in order to secure the information assets. The information security is not just the technical part but how the technical part is used by the human counter-part. This is the baseline of this paper and many other researches being done in this field. The actual implementation of policies is on the employees of the organization. This is what technology is for, to make the human's task easier. It needs the support of humans in order to work. Earlier, the information security was considered from the technical context. However, studies by Chang and Ho, Knapp et al., Ezingeard and Bowen-Schrire, Ma et al., Hu et al., Whitman and Mattord, Philips, Nader et al. suggests the role of managers in maintaining the information security of organizations. The studies have been summarized in Figure 1.

Top management takes all the important decisions regarding formulating security policies and mechanisms which in turn depend on the nature of the organization. Apart from this, they are also responsible for the implementation of these policies. This involves training, motivation and support systems for the employees. Management's attitude and behavior affects the behavior of low level employees. Their commitment and attachment to the organization's faith goes a long way in shaping the employees' activities and roles.

B. SECURITY POLICIES, TRAINING AND AWARENESS

Managerial practices play a significant role in information security process. These practices are policy formulation and training of employees regarding awareness and policy compliance. The security policies remain futile unless the training and awareness programs are implemented by the management in order to make the employees aware of the security culture framework. A more holistic approach towards security will bring huge benefits to the organization. A security policy is needed so that the employees should know the importance of security of information assets. A training program will facilitate this implementation as the employees will know how to carry out the policy. Training changes the attitude and behavior of employees towards compliance of security policies. It also warns them of the various consequences of policy violations.

C. ROLE OF EMPLOYEES

The humans in an organization play a significant part in its progress. Quintessentially, they can shape the direction in which the organization will move. If the employees are sincere and loyal, they will conform to all security policies and trainings in order to safeguard the information of their organization. Adversely, if the employees have a malicious intent and steal information or violate the policies, then they pose the biggest threat to an organization's information security. This is the job of the management to tap the potential of its employees and train them towards achieving a more secure environment in the organization. The management needs to monitor the activities of its employees and control their behavior in case it exhibits doubts about their intentions. Figure 2 highlights the researchers' view of the role of humans in information security of an organization.

Compliance trainings have shown immense improvements in the attitude of the employees. As research suggests that a large percentage of breaches in security happen due of ignorant employees, organizations are spending time and money to formulate and implement the policies

Author	Comments
Chang and Ho	An organization should have a firm management structure and practices to establish information security
Knapp et al.	Support of Top management is most crucial aspect of information security
Ezingeard and Bowen-Schrire	Participation of top management in information security measures leads to improvements in the organization's security levels.
Ma et al.	Management support is the most crucial part of effective information security
Hu et al.	Involvement of top management has a significant effect on the attitude and behavior of employees towards information security compliance
Whitman and Mattord	Security of Information assets is the responsibility of top management
Philips	Management activities have a significant role in effectiveness of information security
Nader et al.	Cooperation and coordination of managers is a source of strength of security measures
Zahoor Ahmed et al.	Information security needs a holistic approach in management context, it's role in information security activities can enhance information security management

Fig. 1 Literature related to Role of Managers in Information Security

Author	Comments
Trcek et al.	Humans are the most important aspect of information security systems
Yeniman et al.	Human factor proves to be the weakest link in information security due to its carelessness about compliance
Rhee, Ryu and Kim	For information security to be effective, the role of humans has to be considered along with advances in technology vertical
Vance et al.	Insiders with malicious intent are a bigger threat than outsiders in organization's information security
Jaeger	Employees are a bigger cause of threat to information breaches than hackers
Nader et al.	Humans are the weakest link but through cooperation and coordination can prove to the biggest strength
Nader, Rossouw and Steven	Commitment and personal norms affect employees' attitude which in turn affects the information security levels

Fig. 2 Literature related to Role of Human aspects in Information Security

keeping them in mind. Again, a holistic approach is needed in order to exploit the maximum out of the information security system. Humans can act as the strongest part of security mechanism if correctly managed and also the weakest link otherwise.

CONCLUSIONS

Information Security is a major concern of all organizations, especially the online businesses. The focus of researchers has been on the technological aspect of information security and many policies have been suggested and adopted over time. However, the role of humans in the security model has been neglected. Any policy can be rendered useless if it is not efficiently implemented by the managers and employees of the organization. This paper highlights their role in the organizational performance and progress. Human resource management is the job of top level managers which need to train and divert their interests in the direction of organization's growth.

REFERENCES

[1] Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. Industrial Management &Data Systems, 106(3), 345–361.

[2] Knapp, K. J., Marshall, T. E., Rainer, R. K., Jr., & Morrow, D. W. (2006). The top information security issues facing organizations: what can government do to help? Network Security, 1, 327.

[3] Ezingeard, J., & Bowen-Schrire, M. (2007). Triggers of change in information security management practices. Journal of General Management, 32(4), 53–72.

[4] Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences, 43(4), 615–660.

[5] Ma, Q., Schmidt, M. B., & Pearson, J. M. (2009). An integrated framework for information security management. Review of Business, 30(1), 58–69.

[6] Whitman, M. E., & Mattord, H. J. (2012). Information security governance for then on-security business executive. Journal of Executive Education, 11(1), 97–111.

[7] Phillips, B. (2013). Information technology management practice: impacts up on effectiveness. Journal of Organizational & End User Computing, 25(4), 50–74.

[8] Safa, Nader Sohrabi, Rossouw Von Solms, and Lynn Futcher. "Human Aspects of Information Security in Organisations." *Computer Fraud & Security* 2016.2 (2016): 15-18. Web.

[9] Soomro, Zahoor Ahmed, Mahmood Hussain Shah, and Javed Ahmed. "Information Security Management Needs More Holistic Approach: A Literature Review." *International Journal of Information Management* 36.2 (2016): 215-25. Web.

[10] Trcek, D., Trobec, R., Pavesic, N., & Tasic, J. F. (2007). Information systems security and human behaviour. Behaviour & Information Technology, 26(2),113–118.

[11] Yeniman, Y., Ebru Akalp, G., Aytac, S., & Bayram, N. (2011). Factors influencing information security management in small-and medium-sized enterprises: a case study from turkey. International Journal of Information Management, 31(4),360–365.

[12] Rhee, H., Ryu, Y. U., & Kim, C. (2012). Unrealistic optimism on information security management. Computers & Security, 31(2), 221–232.

[13] Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. Journal of Management Information Systems, 29(4), 263–290.

[14] Jaeger, J. (2013). Human error, not hackers, cause most data breaches. Compliance Week, 10(110), 56–57.

[15] Safa, Nader Sohrabi, Rossouw Von Solms, and Steven Furnell. "Information Security Policy Compliance Model in Organizations." *Computers & Security* 56 (2016): 70-82. Web.

[16] Alhogail, Areej. "Design and Validation of Information Security Culture Framework." *Computers in Human Behavior* 49 (2015): 567-75. Web.