Chapter 6
A Model of Human Factors in Cyber Security

Maryam Ebrahimi
https://orcid.org/0000-0001-5837-8864
University of Bayreuth, Germany

ABSTRACT

Data has become the new trading currency in today's competitive environment. The human factor is still seen as a significant threat through social engineering channels, despite the advanced technological controls implemented by organizations. Companies can implement appropriate technical solutions, but they are still unable to control the human factor. The aim of the chapter is to better understand the role of human factors in information security. For this purpose, it provides a model that focuses on human-security elements including management commitment, skills, experiences, self-efficacy of human resources, and security culture and training as the vulnerable factors in information security issues. Quantitative methodology and statistical technique are used for analysis. Thus, the main contribution of this research is to present a model of human resource factors in information security that can be applied in several case studies, and the results can be compared.

INTRODUCTION

In today's business, information is recognized as a company's capital and the protection of information and information systems of the organization is one of the important pillars of its survival. The globalization of the economy has created global competition and many companies for the sake of the presence in the global arena have to cooperate with other companies. Thus, the classification, valuation

DOI: 10.4018/978-1-7998-8235-0.ch006

and protection of information resources of the organization (both in the information system and members of the organization) is very vital and important.

Given the modern national economies that are completely dependent on information technology for survival, today the need for information security and information systems is inevitable (Schou and Trimmer, 2004). Numerous national surveys have adapted a large number of attacks on the organization's intelligence resources (Bagchi and Udo, 2003; Gordon et al., 2004; CERT, 2004). Between 1998 and 2003, the number of accidents reported to the US Computer Emergency Response Team almost doubled each year, to which must be added the 529,137 accidents reported in 2003 alone. Management must pay close attention to security in order to maintain and protect organizational information and information systems.

FBI and Crime Scene Investigation in 2008 in respect of cybercrime and security showed that viral attacks were a major cause of financial loss, and that hacking-related incidents had become increasingly common in recent years. Although most respondents to this survey believed in the importance of end-user awareness, many organizations did not provide the necessary training resources. According to the National Cyber Security Alliance in Symantec Home User Study in 2008, 68 percent of users surveyed said they kept sensitive information such as personal, financial and health records on their home computers, 74 percent said they used the Internet for activities such as banking, stock trading, and browsing their personal medical information. In other words, people constantly have access to their banking, financial, and medical records from their computers, which are themselves vulnerable to cyber security threats. Accordingly, organizations have recently been exposed to information security risk, whereby they take preventive measures to maintain organizational information security and control risk. Today, employees use different locations to access organizational information through their mobile phones. Changes in working conditions, especially in crises such as Corona, allow employees to access organizational information by working remotely from their homes. Email-based communication with its attachments is another threat to inbound and outbound traffic (Hazari et al., 2008).

Information security knowledge is essential for all employees or users according to their needs. A lot of information about information security is available through books, the Internet, magazines, etc., but people do not use this information because (Mittal et al., 2010):

- This is a very difficult and time - consuming to obtain specific useful information from the mass of information.
- Users may not be aware of the importance of information security, since they feel that this is the work of information security staff or the IT department.
- There is lack of motivation in acquiring information security knowledge.